National Défense
Defence nationale

Chef – Service d'examen

SYSTÈME INTÉGRÉ DE CONTRÔLE D'ACCÈS

Novembre 2000

7050-9-10-2 (CS Ex)

Canada

TABLE DES MATIÈRES

PAGE

Annexes :

SYNOPSIS

Ce rapport a pour objet de présenter les résultats d'un examen indépendant d'un projet visant à acquérir un Système intégré de contrôle d'accès (SICA) commun pour la région de la capitale nationale et un Service d'identification de la Défense nationale (SIDN) pour l'ensemble du ministère de la Défense nationale et des Forces canadiennes.

Le système commun tel qu'il a été installé ne remplit pas les fonctions de contrôle d'accès ni d'identification nationale d'une manière satisfaisante pour les utilisateurs. L'ajout de la fonction de SIDN à un système de contrôle d'accès et de surveillance standard disponible sur le marché a donné lieu à la mise au point d'un logiciel particulier au MDN qui nécessite un degré élevé de suivi de la part de l'entrepreneur, que l'on a jugé inabordable. Le projet a également souffert de lacunes au niveau de la définition des exigences, et de sa réalisation en tant que projet de construction mineur plutôt que comme un projet d'acquisition de technologie de l'information. L'escalade des coûts du cycle de vie et l'impossibilité de régler rapidement les préoccupations reliées au rendement (voir Annexe A) sont en partie attribuables à la gestion du système par l'usager plutôt que par la direction responsable des systèmes intégrés de gestion.

Bien que l'entrepreneur ait attesté que les éléments matériels et logiciels du système installé et mis à niveau pendant la durée du contrat étaient parfaitement conformes à l'an 2000, il n'en a pas été ainsi. On a finalement cessé d'exploiter la fonction de contrôle d'accès du système à la fin de 1999, en attendant l'examen d'une voie à suivre appropriée.

À la suite des difficultés considérables auxquelles on a dû faire face pendant les premières étapes du projet, le SMA(Fin SM) a exercé un rôle prépondérant dans la résolution du problème et, en collaboration avec le commandant de l'USFC(O), il a déjà pris plusieurs mesures correctives essentielles, y compris :

- *rétablissement intégral du service le 5 septembre 2000;*
- *désignation d'une autorité technique pertinente au sein du Groupe des finances;*
- *inscription des besoins pertinents en ressources à long terme dans le plan d'activités du Groupe des finances;*
- *adjudication d'un contrat de service de soutien permanent;*
- *élaboration d'une nouvelle politique en matière de contrôle d'accès au QGDN.*

Ces initiatives et d'autres mesures correctives énoncées dans le Plan d'action de gestion (voir Annexe C) devraient raisonnablement permettre de régler les problèmes laissés en suspens.

EXAMEN DU SYSTÈME INTÉGRÉ DE CONTRÔLE D'ACCÈS (SICA)

PARTIE I – INTRODUCTION

CONTEXTE

1.1 En 1994, un projet spécial de besoins divers (BD) a été élaboré en vue d'installer un système automatisé de contrôle et de surveillance dans certains édifices du QGDN avant avril 1995. Ce projet visait à améliorer la sécurité physique tout en réduisant le coût des services de sécurité assurés par le biais d'une passation de marchés. La stratégie consistait à acheter en régime de concurrence une architecture et un logiciel non exclusifs offerts dans le commerce.

1.2 Devant la similitude des données nécessaires sur les cartes d'accès (laissez-passer) et les cartes d'identité du MDN, la direction responsable du Service d'identification de la Défense nationale (SIDN) a par la suite recommandé une initiative permettant de réaliser des économies. Une directive ministérielle a été publiée en vue d'inclure la fonction du SIDN au Système intégré de contrôle d'accès (SICA) de la région de la capitale nationale (RCN) et d'utiliser une seule carte dans les deux cas. Les commandements opérationnels ont été invités à utiliser à leurs propres fins la capacité de stockage de la bande magnétique figurant sur la carte d'identité.

1.3 Le message CANFORGEN 005/95 VCEMD 002 171300Z Janvier 1995 annonçait l'intention d'accorder un contrat en vue de donner suite à cette décision, d'introduire le nouveau système dans la RCN avant avril 1995, et de remettre une nouvelle carte d'identité à l'ensemble des membres des FC et des employés du MDN. Des objectifs ambitieux prévoyaient l'achèvement et la mise en œuvre du projet avant le 1er avril 1996, et à l'échelle de la RCN, une réduction annuelle de 840 000 $ des frais contractuels en matière de sécurité à compter de l'AF 1995-1996.

1.4 Le SICA a finalement été mis en place en octobre 1997, environ un an et demi après la date cible, et après une période difficile de mise en œuvre du contrat. La valeur d'attribution du marché était évaluée à 2 566 669 $, mais le coût final a atteint 3 592 706,25 $. Plusieurs commandes rectificatives incluaient environ 450 000 $ pour l'adaptation du logiciel et environ 200 000 $ pour la mise en place d'un Système de contrôle de l'accès autonome (SCAA) à la SFC Leitrim, ce qui constituait un besoin supplémentaire.

1.5 Plusieurs problèmes ont surgi, certains litigieux, concernant le caractère adéquat de la sécurité du contrôle d'accès, la viabilité du double usage de la carte d'identité servant aussi de laissez-passer, ainsi que la gestion du cycle de vie et les coûts.

1.6 Ce rapport a pour objet d'évaluer les aspects de la gestion de projet assurée par l'État. Il ne vise pas à poser des jugements définitifs ou des conclusions au sujet de la performance des entrepreneurs et n'est pas conçu pour cela. Toutes les remarques concernant les entrepreneurs sont fortuites et le lecteur doit les tenir pour telles.

OBJET DE L'EXAMEN

1.7 Cet examen avait pour objet d'examiner le projet SICA à la lumière des difficultés d'ordre technique et contractuel éprouvées, en vue de déterminer les questions pertinentes et de faire des recommandations. On a notamment examiné la gestion des risques dans le contexte historique de la démarche d'acquisition, y compris les moyens pris pour assurer la qualité opérationnelle des produits livrés, ainsi que les conditions actuelles.

PARTIE II - OBSERVATIONS ET CONCLUSIONS

LE PROCESSUS D'ACQUISITION DU SICA

Définition des exigences

2.1 Les exigences relativement à un système de contrôle d'accès et de surveillance ont été définies par un entrepreneur, au printemps 1994. Alors que l'étude prévoyait la possibilité d'utiliser une seule carte à des fins d'identification et de contrôle d'accès, l'énoncé de besoins (EB) s'est limité à la fonction du contrôle d'accès. La solution retenue a été un système disponible dans le commerce au coût d'environ 1,5 million de dollars, et une installation rapide à chaque endroit. Les capacités définies ne prévoyaient pas l'utilisation du système à aucune autre fin. Les renseignements transmis aux fournisseurs éventuels pour solliciter des offres n'incluaient donc pas les besoins supplémentaires reliés à une fonction d'identification nationale. Ces besoins supplémentaires nécessitaient entre autre un élargissement de la base de données, passant d'environ 14 000 à 200 000 cartes, des postes éloignés dans l'ensemble du pays et des champs de données particuliers, y compris un code d'empreintes digitales, le type sanguin et une signature numérique. De plus, les besoins reliés à la protection des données du SIDN étaient plus stricts.

2.2 La décision ministérielle d'inclure la fonction du SIDN au potentiel du SICA a entraîné l'inclusion précipitée des nouveaux besoins à la demande de proposition (DP). Il a donc fallu repousser de deux semaines, en janvier 1995, la date limite de remise des soumissions. Deux des quatre soumissionnaires éventuels se sont retirés après avoir formulé diverses plaintes, y compris des allégations selon lesquelles on prévoyait une solution retenue à l'avance, on les forçait à utiliser une technologie révolue, et le besoin commun ne figurait pas dans la demande initiale. Parmi les deux soumissions présentées, une seule a été jugée conforme. Malgré la probabilité de problèmes imminents, il n'y a pas eu d'analyse de risques appuyée sur des documents. Comme le projet excédait le financement des BM approuvé, on a obtenu un prêt de 735 000 $ du fonds d'investissement du VCEMD. Le contrat a été attribué le 9 février 1995, pour une valeur de 2,57 millions de dollars, et le soumissionnaire retenu devait dépenser les deux tiers des fonds (c.-à-d. les fonds reliés aux BD) avant le 31 mars 1995.

2.3 Compte tenu des circonstances, les besoins reliés au SICA/SIDN n'étaient pas bien définis. Pendant toute la période de mise en œuvre du contrat, tous les intervenants (habituellement une vingtaine de personnes) ont donc dû participer à des réunions hebdomadaires pour tenter de les définir. Ils se sont entendus le 25 août 1995 sur un énoncé des travaux qui incluait l'intégration de la fonction du SIDN au SICA. Cette modification a nécessairement majoré le prix du contrat d'environ 20 p. 100. De manière plus significative, en voulant dépenser le plus possible au cours des sept premières semaines, on a reçu certains produits qui ne convenaient pas et qu'il a fallu remplacer prématurément. Une partie de la fonctionnalité, surtout celle du SIDN, ne s'est pas avérée satisfaisante. De plus, outre le fait que

le logiciel du noyau est exclusif, sa personnalisation pour intégrer la fonction d'identification nationale a donné lieu à un produit individualisé qui nécessite un degré peu souhaitable de surveillance et d'intervention de la part de l'entrepreneur.

Logiciel commercial

2.4 Comme on l'avait proposé initialement, le système de contrôle d'accès devait exploiter un logiciel commercial. Toutefois, l'intégration de la fonctionnalité du SIDN avec le logiciel de noyau commercial a mené à la mise au point d'un programme logiciel particulier au MDN.

Article 16
de la LAI
- Enquêtes

De plus, le fournisseur inclut les frais d'entretien d'une réplique du système SICA MDN et l'introduction des mises à niveau essentielles périodiques, rendues nécessaires en raison des changements apportés à l'ensemble de logiciels commerciaux exploités par le système. Outre le fait que le MDN est obligé d'assumer les frais extraordinaires d'entretien d'un logiciel unique mis au point pour son application particulière, la fonctionnalité du SIDN ne satisfait pas les utilisateurs et on lui attribue les problèmes engendrés au niveau de l'efficacité du contrôle d'accès et de la fonction de surveillance. On n'a pas remédié à ces plaintes apparemment minimes, et certaines mises à niveau ont ajouté d'autres facteurs de mécontentement au sujet du SIDN, qui ne sont pas corrigés non plus.

2.5 L'adaptation du logiciel d'un système de contrôle d'accès à des fins d'identification (ce que l'on semble maintenant considérer comme la fonction la plus vitale du SICA) a donné lieu à des lacunes qui n'avaient toujours pas été corrigées, et ce, alors que cela faisait au moins deux ans que l'entrepreneur fournissait un soutien au logiciel en service. Les problèmes reliés au rendement du SIDN mentionnés à l'Annexe A sont une source de mécontentement et ont réduit la confiance dans l'intégrité de la base de données. De plus, la base de données du SIDN est tenue à jour uniquement dans le serveur principal du SICA. Toutefois, bien qu'il n'y ait pas de redondance en ligne, le système peut sauvegarder le logiciel d'application et les données opérationnelles sur bande magnétique. Le nombre de fichiers est important (plus de 240 000) et augmente rapidement car il faut conserver chaque fichier pendant cinq ans après le départ des intéressés, y compris les membres de la Force de réserve et le personnel d'entrepreneur.

Conclusions

2.6 L'incapacité de bien définir les exigences fonctionnelles et opérationnelles était un facteur de risque directement responsable du peu de possibilités offertes et de la faible concurrence, des retards dans la mise en œuvre, des frais supplémentaires, et de la livraison d'un produit qui s'est révélé insatisfaisant. Lorsque les besoins ont changé, il aurait fallu prendre le temps de veiller à ce que tous les aspects soient bien définis avant de lancer la DP. On semble

avoir sous-estimé les répercussions du changement au niveau des exigences. Une analyse appropriée des risques aurait permis de déterminer l'incidence des facteurs de risques qui existaient.

2.7 L'ajout ultérieur des besoins reliés au SIDN dans le cadre du projet de SICA a nécessité la modification du logiciel commercial proposé. Cette modification a engendré une série de problèmes comme ceux qui sont énumérés à l'Annexe A, et qui subsistent à l'heure actuelle. Lorsque le plan de mise en œuvre de ce projet s'est axé vers la modification d'un logiciel commercial pour y inclure des fonctions supplémentaires, il aurait fallu réévaluer les facteurs de risques. La reconnaissance des travaux de mise au point aurait permis de déterminer les répercussions potentielles sur les risques, le calendrier, les besoins en ressources, et le coût du cycle de vie. Cette démarche aurait alors permis de se rendre compte qu'en fait, la stratégie d'achat avait changé, et qu'il fallait traiter le projet comme un projet d'acquisition d'immobilisations en TI.

2.8 La séparation de la fonction de SIDN du SICA pourrait être une solution intéressante si elle permettait d'exploiter et d'entretenir les systèmes sans dépendre d'un soutien logiciel coûteux et de liens électroniques protégés avec le fournisseur de logiciels. Étant donné que le SICA canadien a été personnalisé de manière à assurer l'intégration du SIDN, il faudra peut-être procéder à une enquête technique pour déterminer s'il est possible de faire à nouveau du SICA un système de production de laissez-passer, de contrôle d'accès et de surveillance au moyen du logiciel de noyau commercial, et les coûts que cela pourrait représenter. Il serait bon de voir si l'on pourrait produire à l'aide de PeopleSoft un rapport personnalisé susceptible de répondre à la nécessité d'une carte d'identité nationale.

GESTION DU CYCLE DE VIE

Structure organisationnelle du projet

2.9 Le projet SICA a été conçu par la division de Sécurité et police militaire (SEPM) de la RCN, qui en a assuré la gestion au cours des premières et des dernières étapes. Le système n'a jamais été officiellement mis à la disposition de la direction chargée de l'administration et de l'exploitation des systèmes [DSI(Fin SM)] ni accepté par cet organisme. Le soutien a donc été assuré pendant environ deux ans de façon ponctuelle. De plus, il n'est pas financé d'une manière appropriée, les coûts sont déraisonnablement élevés, les rôles et les responsabilités n'ont pas été définis, et jusqu'en juin 1999, les décisions étaient prises unilatéralement par l'administrateur de projet de la SEPM RCN.

2.10 La confusion qui règne dans la gestion de ce projet est attribuable aux décisions relatives à la nomination des principaux intervenants, Ainsi, le chef de projet du MDN, à savoir le commandant de l'USFC(O), exerçait au départ le rôle d'administrateur de projet. L'officier supérieur du SEPM, puis l'officier responsable du SMA(IE) lui ont rapidement succédé. En outre, on n'a pas consulté les spécialistes en technologie de l'information (TI) au cours de la

définition initiale des besoins ou de l'évaluation des soumissions. On y a remédié par la suite au cours de la mise en œuvre, en engageant des employés expérimentés en TI et en désignant l'un d'eux à titre d'administrateur de projet. Peu après le départ à la retraite de l'administrateur de projet en 1997, avant l'achèvement des travaux, un officier de la police militaire n'ayant pas la même expérience a assumé les fonctions d'administrateur de projet. Le rôle de responsable du contrat a été confié à Construction de Défense Canada (CDC). Il n'était pas très approprié de gérer ce projet comme un petit projet de construction plutôt que comme un projet d'acquisition de TI, et aucun des gestionnaires de contrat successifs de CDC ne possédait l'expérience pertinente pour traiter avec des fournisseurs de TI, comme des agents des approvisionnements en TI de TPSGC auraient normalement été en mesure de le faire. Ainsi, le contrat n'incluait pas de clause d'indemnité pertinente, et la seule solution en cas de négligence était la résiliation. Des plus, les questions relatives aux droits de propriété, à la prise en charge et au permis d'utilisation du logiciel n'étaient pas claires dans le contrat, pas plus que dans l'énoncé des travaux rédigé par la suite. Les lacunes de ces deux contrats sont ressorties pendant la mise en œuvre du contrat, et la propriété du logiciel ainsi que les droits aux données du code-source sont maintenant des enjeux graves, susceptibles de coûter très cher.

Soutien informatique permanent

2.11 e en œuvre, le système a été mis officieusement à la disposition de l'administrateur de projet de la SEPM, plutôt qu'à l'agence exploitante des systèmes de TI concernée. Le soutien du cycle de vie du SICA a failli flancher au cours de notre examen, vu l'absence d'un concept et d'un plan de soutien reconnu et financé. En attendant un contrat approprié en matière de soutien, l'entrepreneur a prolongé de six mois le soutien assuré pendant la période de garantie du logiciel. À compter du 1er mai 1999, sans qu'il y ait eu d'offre à commandes ou de pouvoirs délégués de TPSGC en matière d'achat, la SEPM et le titulaire du contrat de mise en œuvre ont conclu à tort un accord amiable de trois mois en matière de soutien, pouvant se prolonger chaque mois en attendant la signature d'un contrat. Selon nos constatations, on a omis de définir par écrit les rôles, les responsabilités et les services à livrer pour le prix convenu. L'État versait donc 59 700 $ par mois, plus la TPS, pour un soutien matériel et logiciel non défini.

Article 20 de la LAI – Renseignements de tiers

Le coût des appels de service, y compris l'entretien préventif occasionnel des dispositifs mécaniques, s'élevait à 125 $ l'heure avec un tarif minimum d'une heure. Il revenait à l'État de fournir ou d'acheter des pièces de rechange. Cette situation malencontreuse s'est produite même si l'on savait pertinemment dès le début du projet qu'il serait essentiel de conclure un contrat de soutien informatique permanent, et que les frais annuels de soutien pourraient atteindre près de 320 000 $. En février 1999, chacune des deux entreprises concurrentes d'Ottawa en mesure d'assurer le soutien continu du SICA a

présenté des propositions non-officielles de plus de 400 000 $ par année.

2.12 Le serveur SICA de l'édifice Louis-Saint-Laurent (LSL) a subi une défaillance catastrophique au cours de la fin de semaine du 3-4 juillet 1999, apparemment à cause de la foudre et d'une mise à la masse insuffisante. L'administrateur de projet du SICA était réticent à financer la réparation du serveur en attendant des décisions sur la voie à suivre. Le technicien de l'entrepreneur qui comprenait le SICA était en vacances en juillet, le dernier mois de l'accord amiable. En fait, au moment de notre examen, l'entrepreneur n'avait pas soumis de facture pour le soutien logiciel assuré en juillet. D'autre part, l'administrateur de projet avait obtenu de l'entrepreneur le 16 février 1999 une offre de prix de 5 490 $, plus la TPS, pour réinstaller le serveur et l'ordinateur nodal de contrôle d'accès dans une pièce réservée au serveur. Bien que le déménagement ne se soit jamais concrétisé, l'entrepreneur a soumis une facture pour les travaux, laquelle n'a évidemment pas été payée. Le serveur était encore hors service le 24 mars 2000, et trois autres agents de sécurité du secteur privé ont été employés sur les lieux pendant les heures de travail à compter du début de juillet 1999. Si le serveur avait été installé correctement à l'endroit initial, ou réinstallé comme prévu au printemps 1999, ces dépenses imprévues n'auraient pas été nécessaires.

Logiciel exclusif – Implication contractuelle

2.13 L'administration du SICA par des employés qui ne sont pas des spécialistes des systèmes d'information a laissé l'État à la merci de prétentions potentiellement exagérées ou injustifiées à l'égard d'un « logiciel exclusif ». L'entrepreneur ne détient pas lui-même les droits de propriété. En fait, le propriétaire du logiciel a confié à une autre entreprise d'Ottawa les droits exclusifs de distribution de ses produits au Canada. Nous avons examiné la question avec des agents d'approvisionnement en TI de TPSGC qui étaient au courant de la situation en ce qui concerne le SICA et de la nécessité d'un contrat de soutien permanent. Selon TPSGC, il semblait y avoir, en août 1999, deux fournisseurs soutenus par le propriétaire du logiciel et en mesure d'offrir un prix concurrentiel. Ils auraient eu alors l'intention d'annoncer publiquement l'invitation à soumissionner.

2.14 Le logiciel qui constitue le noyau du SICA est effectivement exclusif, et l'État l'a reconnu au moment de s'entendre sur l'énoncé final des travaux (ET) en août 1995. Toutefois, la partie du SICA affectée au SIDN devait avoir la souplesse voulue pour s'adapter aux changements législatifs, organisationnels et autres, et permettre à l'utilisateur de produire des écrans de cartes d'identification sur mesure. Il est donc prévu dans l'ET que le code source de l'élément informatique particulier au MDN soit donné au MDN, et que celui-ci possède le droit d'auteur concernant ce logiciel. Néanmoins, en raison de l'intégration de la fonctionnalité du SIDN à la fonctionnalité essentielle du logiciel de noyau, l'État n'a guère la possibilité de manipuler le code source. De plus, on ne sait pas si le fait de séparer la fonction de SIDN du SICA aura pour effet de retirer du SICA autre chose que l'ensemble de la base de données du SIDN. Rien ne prouve que le code source du logiciel particulier au MDN a de fait été remis au MDN.

Conformité à l'an 2000

2.15 L'entrepreneur principal a attesté par écrit le 20 février 1997 que l'équipement et le logiciel d'origine du SICA/SCAA, et toutes les mises à niveau, fournis en vertu des modalités du contrat étaient parfaitement conformes à l'an 2000. Toutefois, en 1998, l'initiative A2K du MDN a permis de déterminer que le système n'était pas conforme. Sans demander aide et conseils auprès du personnel SIG concerné, de l'ancien responsable du contrat de CDC, ou de TPSGC, l'administrateur du projet SICA de la SEPM a entrepris de remplacer le matériel et le logiciel en s'adressant à l'entrepreneur principal initial. Alors que cela n'était pas prévu ni inscrit au budget, on a dépensé environ 133 000 $ jusqu'à maintenant pour assurer la mise à niveau du SICA/SIDN et du SCAA. L'installation du nouveau matériel et du logiciel révisé a été interrompue en juillet 1999 en raison de l'arrivée en poste d'un nouvel administrateur de projet et d'imprécisions au sujet d'une entente amiable provisoire concernant le soutien logiciel permanent. L'indécision à propos de l'utilisation future du SICA et les vacances prises par les techniciens TI de l'entrepreneur ont empiré les choses, de sorte qu'en juillet 1999, on a perdu trois semaines de travail potentiel de la part de l'entrepreneur. L'important dépassement budgétaire au niveau de la SEPM a également contribué à retarder une décision visant à obtenir un financement pour remédier au problème de soutien. En décembre 1999, une expertise technique a confirmé que les noyaux SICA/SCAA appelés modules d'interface de sous-système, et que les dispositifs de chiffrement installés partout n'étaient pas conformes et que le système risquait de tomber en panne. L'approbation de financement a été obtenue trop tard pour que l'on puisse adjuger le marché au fournisseur de logiciel afin de régler le problème avant le 31 décembre 1999.

Conclusions

2.16 Les changements successifs d'administrateurs de projet et de responsables du contrat ont favorisé une confusion évitable. L'impossibilité d'obtenir l'avis de spécialistes en TI au cours de la phase de définition des besoins et de recourir aux connaissances spécialisées de TPSGC en matière d'approvisionnement en TI sont deux omissions graves qui ont donné lieu à des clauses contractuelles mal définies.

2.17 Le soutien informatique permanent du SICA ne peut être assuré que par le biais d'une gestion confiée à une équipe compétente en TI, et par le financement d'un soutien assuré par l'entrepreneur. La détermination de ces exigences devrait toutefois faire partie d'une évaluation technique visant à définir la voie à suivre qui convient.

2.18 Selon TPSGC en ce qui concerne l'approvisionnement en TI, il ne semble pas y avoir d'empêchement juridique à lancer un appel d'offres visant à adjuger un contrat d'assistance à l'égard du SICA, mais les entreprises candidates doivent obtenir un accord d'autorisation de la part du propriétaire du logiciel. Toutefois, puisque le fournisseur de logiciels a indiqué qu'il a

choisi un distributeur exclusif au Canada, il est permis de douter, à l'heure actuelle, de sa bonne volonté à appuyer encore l'entrepreneur principal désigné initialement.

2.19 Le matériel et le logiciel fournis initialement ne sont certes pas conformes à l'an 2000. Malgré une enquête urgente menée par le MDN en consultation avec le fournisseur de logiciels en décembre 1999, on n'a pas eu le temps de régler les problèmes. Le matériel et le logiciel mis à niveau qui ont été partiellement installés n'ont pas suffi à éviter la défaillance du système de contrôle d'accès du SICA le 1er janvier 2000.

POLITIQUE ET CONDITIONS DE SÉCURITÉ

2.20 Le document de politique, Instruction du QGDN - DGSM 5/92, Politique de contrôle de l'accès – Immeubles du Quartier général de la Défense nationale, est antérieur au SICA d'environ cinq ans, et l'on reconnaît qu'il est dépassé. De plus, les dispositifs visant à augmenter la sécurité du SICA ne sont pas pleinement exploités. Ainsi, le potentiel de surveillance d'accès, y compris le dispositif antirépétition ainsi que les alarmes et les rapports sur l'état de la carte (p. ex., périmée, endommagée, perdue/volée, numéro d'identification personnelle erroné) n'est pas employé efficacement.

2.21 Avant l'installation du SICA et des tourniquets, la sécurité reposait sur la vigilance d'agents de sécurité chargés d'observer les divers types de laissez-passer que l'on porte. L'efficacité de cette méthode est toujours incertaine, surtout en période de pointe. Le projet SICA avait donc pour objectif d'assurer, au moyen de l'informatique, une sécurité accrue à moindre coût. Les facteurs dont on a tenu compte pour retenir la solution du SICA incluaient l'aspect esthétique des entrées principales, et le souci de ne pas dépasser les exigences minimales en matière de sécurité fixées par le Conseil du Trésor. Toutefois, puisqu'il était reconnu que l'on pouvait facilement contourner les tourniquets et les barrières fixes installés aux entrées des édifices, le plan de sécurité et les prévisions de coût initiaux du SICA incluaient des gardes de sécurité. En ce qui concerne les édifices Pearkes et LSL, le plan incluait des gardes postés près des tourniquets, car les cabines de réception/sécurité de l'étage principal ne sont pas suffisamment près des barrières pour permettre une surveillance adéquate de la circulation du personnel. Après l'installation du SICA, les allocations budgétaires sévèrement réduites ont entraîné le retrait des gardes de sécurité aux tourniquets d'entrée principale, car les objectifs d'économie imposés depuis peu allaient au-delà de ce qu'on prévoyait au départ. Récemment, en partie en raison des défaillances du système SICA, et du fait que certains organismes clients n'acceptaient pas le niveau de sécurité assuré, le retour des gardes aux tourniquets a contribué à augmenter les dépenses reliées à la sécurité prévues dans l'entente. Il y avait, et il y a encore, des perceptions différentes au sujet des mesures qui offrent une sécurité suffisante.

2.22 La Politique de sécurité du ministère de la Défense nationale (PSMDN) confère aux commandants et aux cadres supérieurs un pouvoir et un contrôle à l'égard de la conception, de la mise en œuvre et de la répartition des ressources relatives aux mesures de protection. La gestion des risques en matière de sécurité a pour objectif de fournir en matière de sécurité une solution rentable qui ramène le risque résiduel pour le Ministère à un niveau acceptable. Les conseillers

en sécurité de formation et d'unité doivent répondre aux commandants et aux cadres supérieurs de l'application d'une méthodologie de surveillance de la menace et des risques permettant de déceler les risques et les points faibles, et d'effectuer une analyse coût-avantage des mesures de sécurité. Dans l'exercice de cette responsabilité, le GP RCN a mis le commandant de l'USFC(O) au courant des lacunes associées au SICA et à l'utilisation de la carte d'identité nationale comme laissez-passer. Toutefois, les demandes officielles de directives sur la politique et les conditions de sécurité adressées par la SEPM (24 février 1998, 17 novembre 1998 et 20 avril 1999) sont restées sans réponse. La mesure prise en ce moment pour régler de toute urgence les problèmes de gestion fonctionnelle du SICA et du SIDN devrait clarifier la voie à suivre, et permettre de remplacer l'Instruction du QGDN - DGSM 5/92, Politique de contrôle de l'accès – Immeubles du Quartier général de la Défense nationale.

Conclusion

2.23 Il est nécessaire d'apporter des éclaircissements à la politique sur les conditions de sécurité au niveau local en vue de déterminer la voie à suivre pour veiller à la sécurité dans les installations du MDN situées dans la RCN. Parmi les questions en suspens, il faut notamment déterminer s'il convient ou non :

a. de séparer la fonction de SIDN de la fonction et du système SICA;

b. d'adopter un système de laissez-passer caractéristique et bien visible, différent de la carte d'identité nationale;

c. d'assurer une supervision aux tourniquet dans les entrées principales des édifices Pearkes et LSL;

d. à long terme, de remplacer les tourniquets déjà anciens par un type plus efficace de barrière aux entrées principales.

2.24 Il faudrait envisager une utilisation plus efficace du potentiel de surveillance centralisée du SICA, y compris l'élaboration d'instructions permanentes d'opération pour assurer des mesures appropriées de relance des alertes et des rapports.

MESURES CORRECTIVES DU GP RCN ET DE L'USFC(O)

2.25 Vu l'urgence perçue de la situation, l'équipe d'examen a présenté un exposé au GP RCN le 14 octobre 1999, en lui faisant part des observations et des recommandations préliminaires, lesquelles ont toutes été entérinées et figurent dans ce rapport. Le GP RCN a ensuite demandé officiellement à l'USFC(O) et au DSI (Fin SM) le pouvoir et les ressources nécessaires pour entreprendre une intervention urgente visant à régler les problèmes les plus pressants (note de service 5450-2 (GP), 28 octobre 1999). L'enquête technique qui a suivi et les discussions avec le fournisseur de logiciels ont permis d'établir qu'il manquait de temps pour régler la vulnérabilité

à l'A2K avant l'échéance du nouvel an. Il a donc été convenu le 17 décembre 1999 d'exploiter séparément la fonction du SIDN, et de cesser d'exploiter la fonction de contrôle d'accès du SICA à la fin de l'année en attendant les décisions découlant d'une étude rationnelle de tous les facteurs. La réponse de la direction, présentée à la page 13, contient des renseignements détaillés sur l'intervention prévue et les premiers résultats obtenus.

PARTIE III - RECOMMANDATIONS

Recommandations particulières au SICA

3.1 Il est recommandé que le GP RCN consulte le personnel du DSI(Fin SM) et du SMA(RH- Mil) et collabore avec lui pour résoudre les problèmes suivants :

a. potentiel et acceptabilité de PeopleSoft pour assumer les fonctions de registre et de carte d'identité de la Défense;

b. enquêter sur la viabilité technique d'un retour au logiciel commercial pour un système de contrôle d'accès et de surveillance;

c. en supposant que l'on décidera de conserver un système de contrôle d'accès et de surveillance exploitant le matériel et le logiciel commercial existants, entreprendre le processus nécessaire pour obtenir un soutien informatique permanent, et s'il y a lieu, la configuration du logiciel commercial.

3.2 Il est également recommandé que le GP RCN :

a. en consultation avec le DSI(Fin SM), déclare aux supérieurs les besoins immédiats et futurs en soutien financier;

b. mette le système à la disposition du DSI(Fin SM) en vue de l'exploitation technique et pour obtenir en bout de ligne une aide financière pour l'avenir.

3.3 Il est recommandé que l'USFC(O) définisse une nouvelle politique en matière de contrôle d'accès et de surveillance, ou apporte des éclaircissement à la politique en vigueur, à la lumière d'une utilisation réaliste du potentiel informatique, et remplace ensuite l'Instruction du QGDN 5/92, Politique de contrôle de l'accès – Immeubles du Quartier général de la Défense nationale.

Recommandations générales

3.4 Le personnel de gestion du projet et du cycle de vie devrait être sensibilisé aux répercussions possibles au niveau des risques et de la mise en œuvre qui sont associées à des changements de stratégie en matière d'approvisionnement (p. ex., passer d'un logiciel commercial à la conception), et doit donner suite à ces changements en réexaminant d'une manière appropriée l'évaluation des risques, le coût, le calendrier et s'il y a lieu, les exigences de rendement.

3.5 Le soutien informatique permanent après livraison doit figurer dans le plan stratégique concernant l'acquisition d'équipement, y compris les projets relatifs aux besoins divers.

Réponse de la direction

3.6 Le SMA(Fin SM) a confié au DSI(Fin SM) la responsabilité de l'exploitation et de l'entretien du SICA/SCAA et du soutien du SIDN qui y est associé. L'USFC Ottawa utilise les systèmes; le GP RCN ainsi que le SIDN continueront d'assurer la garde des données. Les nouvelles fonctions ou les nouvelles exigences doivent être définies par le client, le GP RCN, avant la mise en œuvre d'une solution technique par le fournisseur de service.

3.7 On a entrepris du travail d'état-major en vue d'examiner les solutions offertes en ce qui concerne la fonction du SIDN, y compris la possibilité d'employer PeopleSoft. L'autorité technique fait toutefois observer que s'il faut un code personnalisé pour interfacer le SIDN et PeopleSoft, il faut comprendre qu'il pourrait en découler des risques inacceptables. Parmi les solutions disponibles, il faut donc envisager la possibilité d'exploiter un autre logiciel spécialisé d'identification standard disponible sur le marché.

3.8 L'autorité technique collabore avec le fournisseur de logiciels d'origine et des spécialistes en logiciel du secteur privé engagés sur place pour déterminer la meilleure solution technique applicable aux systèmes de contrôle d'accès, au SICA et au SCAA. La solution technique finale est un système abordable basé sur un logiciel commercial.

3.9 Le DSI(Fin SM) fait observer qu'aucun des systèmes associés au SICA/SIDN et au SCAA n'a été reconnu conforme aux normes de sécurité du MDN et des FC. Les responsables comptent s'occuper du certificat de sécurité lorsqu'ils examineront ces systèmes.

3.10 La Politique de contrôle de l'accès a été redéfinie à la lumière des recommandations de ce rapport, dans une version préliminaire de la Directive sur la sécurité n^{o} 7 – Contrôle d'accès au QGDN (Annexe D).

3.11 Le plan d'action de l'Annexe C, ainsi que l'Annexe D, examine en détail les progrès accomplis jusqu'à maintenant et présente une manière de résoudre les points encore en litige. Le SICA est redevenu entièrement opérationnel le 5 septembre 2000.

SUJETS DE MÉCONTENTEMENT À L'ÉGARD DU SICA/SIDN

PRÉOCCUPATIONS GÉNÉRALES

1. L'intégration du système de carte d'identité nationale et du système local de laissez-passer de la RCN n'a été utile à aucune de ces fonctions. La carte d'identité du MDN ne permet pas nécessairement à son détenteur d'avoir accès à n'importe quelle installation du MDN, mais le double usage de la carte en donne l'impression. La carte d'identité ne présente pas les traits caractéristiques très apparents qui sont habituels à un laissez-passer.

2. L'utilisation de la carte d'identité à titre de laissez-passer nécessite quotidiennement de nombreux balayages, ce qui entraîne une détérioration rapide de la carte au point de la rendre inutilisable comme carte d'identité. Dans la RCN, le remplacement prématuré des cartes à mi-chemin ou moins de la période d'expiration de cinq ans, est donc devenu chose courante.

3. Étant donné qu'en vertu du protocole international relatif aux cartes d'identité, celles-ci ne doivent pas être altérées de quelque manière que ce soit, y compris par des perforations, il est nécessaire, pour pouvoir les utiliser comme laissez-passer et les montrer en tout temps, de les insérer dans une pochette ou un portefeuille. Cela augmente à la fois les frais d'émission et les risques de perte de cartes d'identité.

SIDN

4. La fonction de SIDN s'exécute au moyen d'un serveur principal partagé par le SICA. Il n'y a pas de sauvegarde en ligne. Les employés du SIDN sont sensibilisés au double danger associé à une défaillance du système et à sa vulnérabilité, vu l'accès constant du lecteur de carte au serveur principal. La défaillance du serveur principal du SICA/SIDN peut notamment avoir pour conséquence l'impossibilité d'accéder à la base de données nationale d'identification du personnel et l'incapacité d'imprimer des cartes, ce qu'il est souvent urgent de faire en prévision des déploiement opérationnels. Ce n'est plus une situation hypothétique; le serveur principal est tombé en panne en novembre 1999 et il est demeuré hors service plusieurs jours. Certains facteurs précis de mécontentement sont énumérés ci-après :

- impossibilité d'effectuer une annulation de bloc, fonction nécessaire car les fichiers sont supprimés cinq ans après le départ;

- impossibilité de supprimer des données électroniques de classification dactyloscopique sans effacer l'ensemble du fichier (nécessaire en raison du changement de politique selon lequel les empreintes digitales doivent être retirées des dossiers des employés civils du MDN);

- les opérateurs système n'ont pas la possibilité d'exécuter des fonctions normales de base de données comme le tri, les interrogations ad hoc, la gestion de fichiers et la production de rapports;

- les signatures et les photographies numériques sont transmises sur disquettes et doivent être reliées manuellement aux données du tourniquet, ce qui fait double emploi;

- le système exploite un processus fondé sur le fichier de chaînes de caractères en ce qui concerne les renseignements qui proviennent des unités de campagne; lorsque le dossier d'une personne est retiré du fichier à des fins d'enchaînement, le délai de rafraîchissement de l'écran est en moyenne de 13 minutes et peut prendre jusqu'à 21 minutes;

- le système ne peut pas imprimer des renseignements personnels sur papier à des fins d'examen – seulement sur l'imprimante de cartes;

- les opérateurs ne peuvent pas entrer des changements de configuration (p. ex., de nouvelles imprimantes);

- le problème d'intégrité des données doit être réglé;

- la fonction de la touche Échappement que l'on a perdue pour une raison ou pour une autre au cours de la dernière mise à niveau doit être restaurée.

LISTE D'ACRONYMES

BD	Besoins divers
CDC	Construction de Défense Canada
CS Ex	Chef – Service d'examen
DP	Demande de proposition
DSI (Fin SM)	Directeur – Service d'information (Finances et Services du Ministère)
ET	Énoncé des travaux (accord d'août 1995 entre l'État et l'entrepreneur)
FC	Forces canadiennes
F et E	Fonctionnement et entretien
GP RCN	Grand prévôt de la RCN
PPER	Profil du projet et évaluation des risques
OTAN	Organisation du Traité de l'Atlantique Nord
QGDN	Quartier général de la Défense nationale
RCN	Région de la capitale nationale
SCAA	Système de contrôle de l'accès autonome
SMA(RH)	Sous-ministre adjoint (Ressources humaines)
SEPM	Sécurité et police militaire
SFC	Station des Forces canadiennes
SICA	Système intégré de contrôle d'accès
SIDN	Service d'identification de la Défense nationale
TI	Technologie de l'information
TPSGC	Travaux publics et Services gouvernementaux Canada
USFC(O)	Unité de soutien des Forces canadiennes (Ottawa)

PLAN D'ACTION

OBSERVATIONS ET RECOMMANDATIONS	BPR	ÉTAT/DATE D'ACHÈVEMENT	EXAMEN DE LA QUESTION
1. La personnalisation du logiciel du noyau pour intégrer la fonction d'identification nationale a donné lieu à un produit individualisé qui nécessite un degré peu souhaitable de surveillance et d'intervention de la part de l'entrepreneur. (Page 3/13, para 2.3).	SDI (Fin SM)	Travaux en cours	Le degré de surveillance de la part de l'entrepreneur a beaucoup diminué et le personnel du DSI(Fin SM) a assumé la responsabilité des aspects techniques du système. On a obtenu les lignes de code, et les frais d'entretien sont tombés à 325 000 $ pour la présente AF et devraient diminuer encore pour atteindre 225 000 $ d'ici la prochaine AF. Bien que les frais d'entretien semblent élevés, ils correspondent à la moyenne de l'industrie pour un système informatique qui vaut environ 3,5 millions de dollars.
2. Le maintien → entre le fournisseur de logiciels américain et le serveur principal du QGDN est une source de préoccupation constante → (Page 4/13, para 2.4)	SDI (Fin SM)	Réglé Article 16 de la LAI - Enquêtes	Cette pratique a cessé, → et des employés du SDI(Fin SM) se sont inscrits au cours → pour se spécialiser davantage dans ce domaine.
3. Le fournisseur inclut les frais d'entretien d'une réplique en trois appareils du système SICA du MDN. (Page 4/13, para 2.4)	SDI (Fin SM)	Réglé	Cet aspect ne fait plus partie de notre contrat d'entretien.
4. Le MDN est obligé d'assumer les frais extraordinaires d'entretien d'un logiciel unique. (Page 4/13, para 2.4)	SDI (Fin SM)	Réglé	Nous avons maintenant le code du SIDN.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
5. La fonctionnalité du SIDN ne satisfait pas les utilisateurs et on lui attribue les problèmes engendrés au niveau de l'efficacité du contrôle d'accès et du système de surveillance. (Page 4/13, para 2.4)	GPFC, DSI(Fin SM)	Travaux en cours	Puisque le CGD a décidé d'utiliser une seule carte pour le contrôle d'accès et l'identité, le SIDN demeurera relié au SICA et il sera difficile de répondre à toutes les exigences. Le GP RCN déterminera les lacunes/problèmes ou les nouveaux besoins à l'intention du personnel du DSI(Fin SM), qui prendra ensuite les mesures qui s'imposent. Lorsque la solution sera mise en œuvre, le GP RCN participera à l'essai d'acceptation par l'utilisateur pour s'assurer que le produit livré règle vraiment les lacunes/ problèmes constatés initialement.
6. La base de données du SIDN est tenue à jour uniquement au moyen du serveur principal du SICA. Toutefois, bien qu'il n'y ait pas de redondance en ligne, le système peut sauvegarder le logiciel d'application et les données opérationnelles sur bande magnétique. (Page 4/13, para 2.5)	DSI(Fin SM) Article 16 de la LAI - Enquêtes	Le DSI(Fin SM) doit examiner la situation. ↓	Ces affirmations laissent supposer que la conception initiale est imparfaite; toutefois, cela ne semble pas poser problème d'après l'utilisation actuelle et prévue. Puisque la durée de vie critique de l'identification ne pose pas problème, les sauvegardes semblent suffisantes. On continuera d'examiner la question, mais aucune mesure n'est envisagée pour le moment.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
7. La séparation de la fonction du SIDN du SICA pourrait être une solution intéressante si elle permettait d'exploiter et d'entretenir les systèmes sans dépendre d'un soutien logiciel coûteux et de liaisons électroniques protégées avec le fournisseur de logiciels. (Page 5/13, para 2.8)	DSI (Fin SM)	Réglé Article 16 de la LAI - Enquêtes	À lire à la lumière des para 1 et 2 de cette annexe. Essentiellement, les frais de soutien élevés sont passés de 800 000 $ à 225 000 $ pour la prochaine AF.
8. Il faudra peut-être procéder à une enquête technique pour déterminer s'il est possible de faire à nouveau du SICA un système de production de laissez-passer, de contrôle d'accès et de surveillance au moyen du logiciel de noyau commercial. Il serait bon de voir si l'on pourrait produire à l'aide de PeopleSoft un rapport personnalisé … la carte d'identité nationale. (Page 5/13, para 2.8)	SMA(Fin SM) DSI(Fin SM)	Le DSI(Fin SM) examinera le logiciel commercial d'ici le 15 sept 2001.	On a examiné une proposition de projet du DSI(Fin SM) concernant un système d'identité national distinct, disponible dans le commerce, et pour le moment, on fera en sorte de stabiliser le système existant. Étant donné que les frais d'exploitation du système actuel correspondent à la norme de l'industrie, il n'est pas prévu de séparer le SIDN du SICA. Cette décision sera réexaminée en sept 2001. En ce qui concerne l'interface avec PeopleSoft, on procédera à des vérifications d'ici là pour voir s'il faut un code personnalisé.
9. Le système n'a jamais été officiellement mis à la disposition de la direction d'administration et d'exploitation des systèmes concernée, la DSI(Fin CS). (Page 5/13, para 2.9)	DSI (Fin SM) GP Sécur GP RCN	Réglé	Le DSI(Fin SM) est le propriétaire du système; il est responsable de l'ensemble de la budgétisation et de la passation de marchés concernant l'entretien correctif et préventif et les améliorations du système. Le GP Sécur est responsable de la politique sur la sécurité et le GP RCN exploite le système.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
10. (Page 6/13, para 2.11) Article 20 de la LAI – Renseignements de tiers	Cmdt USFC(O)	Article 21 de la LAI - Avis	Article 21 de la LAI - Avis
11. Le coût des appels de service, y compris l'entretien préventif occasionnel des dispositifs mécaniques, s'élevait à 125 $/h avec un tarif minimum d'une heure. (Page 6/13, para 2.11)	DSI(Fin SM)	Réglé	Le DSI(Fin SM) est la première autorité chargée de régler les problèmes reliés à la TI, contrairement à l'usage qui consistait à signaler immédiatement le problème à l'entrepreneur. Si le DSI(Fin SM) n'est pas en mesure de régler le problème, on consultera les techniciens d'ICS à Houston. Si notre personnel n'était pas en mesure de régler le problème, on consulterait alors Ottawa Security Systems.
12. On ne sait pas si le fait de séparer la fonction de SIDN du SICA aura pour effet de retirer du SICA autre chose que l'ensemble de la base de données du SIDN. (Page 7/13, para 2.14)	DSI(Fin SM)	Aucune mesure nécessaire	Il n'y a pas d'incidence tangible sur le SICA à part celle qui est mentionnée.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
13. Rien ne prouve que le code source du logiciel particulier au MDN a de fait été remis au MDN. (Page 7/13, para 2.14)	DSI(Fin SM)	Réglé	On a obtenu le code source et le personnel du DSI(Fin SM) l'analyse.
14. Le soutien informatique permanent du SICA ne peut être assuré que par le biais d'une gestion confiée à une équipe compétente en TI, et par le financement d'un soutien assuré par l'entrepreneur. (Page 8/13, para 2.17)	SMA(Fin SM)	Réglé	Le DSI(Fin SM) s'assure qu'un soutien spécialisé en TI et des lignes de financement sont indiqués dans le cadre du plan d'activités du SMA(Fin SM).
15. Le matériel et le logiciel fournis initialement ne sont certes pas conformes à l'an 2000. (Page 9/13, para 2.19)	Cmdt USFC(O)	Le cmdt de l'USFC(O) doit vérifier d'ici le 15 nov 2000 si les dispositions contractuelles garantissaient la conformité à l'A2K au moment de l'achat du système.	Bien que l'information contenue dans le rapport ait pour objet d'expliquer la défaillance du système, on fera des recherches pour vérifier si au moment de l'achat, certaines dispositions contractuelles visaient à fournir un système conforme à l'A2K. Selon le CS Ex, puisque la conformité ne figurait pas dans le contrat initial, il n'est peut-être pas possible d'obtenir réparation. L'attestation fournie par l'entrepreneur principal le 20 fév 1997 était erronée. Il faudrait obtenir un avis juridique pour déterminer s'il vaut la peine de demander réparation.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
16. Le document intitulé Politique de contrôle de l'accès – Immeubles du Quartier général de la Défense nationale, est antérieur au SICA d'environ cinq ans, et l'on reconnaît qu'il est dépassé. (Page 9/13, para 2.20)	GP RCN	Réglé	L'annexe D contient une version préliminaire d'une directive sur la sécurité.
17. Il faudrait envisager une utilisation plus efficace du potentiel de surveillance centralisée du SICA, y compris l'élaboration d'instructions permanentes d'opération pour assurer des mesures appropriées de relance des alertes et des rapports. (Page 10/13, para 2.24)	Cmdt USFC(O) DSI(Fin SM)	Le cmdt de l'USFC(O) et le DSI(Fin SM) doivent se rencontrer et examiner les besoins d'ici le 15 nov 2000. Au cours de cette réunion, ils examineront aussi les nouveaux édifices qui seront en ligne sous peu comme le 400, rue Cumberland. Le cmdt de l'USFC(O) et le GP RCN examineront les capacités du système et détermineront les fonctions qui doivent être en service avant le 1er fév 2001.	Bien que l'on ait une compréhension de base des exigences en matière de sécurité, le système SICA peut offrir un potentiel bien supérieur à ce qu'on utilise à l'heure actuelle. On a dressé une liste détaillée des capacités. Il faut une consultation pour examiner l'utilisation des fonctions courantes et déterminer (le cas échéant) les capacités supplémentaires qui devraient être activées. Les premières discussions ont révélé le désir d'inclure les caractéristiques de carte d'identité perdue/volée et de coordination à l'aide d'une caméra vidéo. Il est prévu de rédiger des IPO concernant les capacités que l'on prévoit utiliser dès qu'elles seront définies.

OBSERVATIONS ET RECOMMANDATIONS	**BPR**	**ÉTAT/DATE D'ACHÈVEMENT**	**EXAMEN DE LA QUESTION**
18. Il est nécessaire d'apporter des éclaircissements à la politique sur les conditions de sécurité pour déterminer s'il convient ou non : - d'exercer une surveillance aux tourniquets dans les entrées principales des édifices Pearkes et LSL; - à long terme, de remplacer les tourniquets déjà anciens par un type plus efficace de barrière aux entrées principales. (Page 10/13, para 2.23)	Cmdt USFC(O) DSI(Fin SM) GP RCN	La question de la surveillance à l'entrée est réglée; Le DSI(Fin SM) examinera la possibilité de modifier l'équipement actuel d'ici le 15 nov 2000. Le GP RCN dirigera un examen de l'efficacité des tourniquets actuels d'ici le 15 sept 2001.	La supervision est assurée à ces endroits. Étant donné qu'une surveillance s'exerce aux tourniquets, il est moins nécessaire de remplacer cet équipement. On examinera la possibilité d'allonger les « bras » actuels.
19. Le DSI(Fin CS) fait observer qu'aucun des systèmes associés au SICA/SIDN et au SCAA n'a été reconnu conforme aux normes de sécurité du MDN et des FC. (Page 13/13, para 3.9)	GP RCN DSI (Fin SM)	Le GP RCN et le DSI(Fin SM) doivent assurer la coordination et remplir les documents d'attestation et les transmettre aux autorités concernées d'ici le 31 mars 2001.	Il y a eu des discussions initiales au sujet du processus d'attestation.

RÉGION DE LA CAPITALE NATIONALE

DIRECTIVE SUR LA SÉCURITÉ N^{O} 7 – CONTRÔLE D'ACCÈS AU QGDN

Références : A. A-SJ-100-001/AS-000 PEDN
B. Règlement sur les secteurs d'accès contrôlé relatif à la Défense
C. Règlement sur l'inspection et les fouilles (Défense)
D. 2120-1 (Grand prévôt) 14 avril 1998 (Directive d'orientation provisoire du QGDN)

7.01 GÉNÉRALITÉS

1. Un contrôle d'accès a été mis en place aux principales installations du QGDN dans le but de préserver l'intégrité des zones d'accès réservé et de protéger adéquatement les ressources du MDN et des FC. La portée des mesures réelles de contrôle en vigueur dans certaines installations varie quelque peu mais les protocoles essentiels sont les mêmes dans tous les édifices.

2. Cette directive a pour objet d'énoncer la politique relative au contrôle d'accès au QGDN et les mesures administratives à respecter pour obtenir un laissez-passer et établir des privilèges d'accès.

7.02 POLITIQUE CONCERNANT L'ACCÈS

1. Points d'accès autorisés. Le personnel doit passer uniquement par un point d'accès autorisé et contrôlé pour entrer dans un édifice d'accès contrôlé du QGDN ou en sortir. Un point d'accès autorisé est :

a. une entrée contrôlée par la compagnie de police militaire (cie PM) de l'USFC Ottawa pour en permettre l'accès au public pendant les heures d'ouverture. Ce sont les points d'entrée supervisés/contrôlés d'un édifice qui sont utilisés pour y avoir accès couramment ou quotidiennement;

b. un point d'entrée/sortie différent du précédent que le cmdt de l'USFC Ottawa ou le Grand prévôt (GP) RCN, au nom du cmdt, a permis d'utiliser dans le cadre d'une activité spéciale. Cette disposition s'applique généralement au passage par une porte qui ne sert pas couramment, mais par laquelle on a donné l'autorisation de passer à l'occasion d'une activité ou d'un événement spécial;

c. une sortie de secours qui ne sert qu'en cas d'urgence et par laquelle il n'est pas permis d'entrer/sortir, à moins d'une autorisation en vertu des alinéas 1a ou 1b ci-dessus.

2. Accès aux installations. L'accès aux installations du QGDN se limite aux personnes autorisées à posséder un laissez-passer du QGDN émis en bonne et due forme, et qui ont affaire dans une installation. Le seul fait d'être membre du MDN ou des FC ne confère pas automatiquement le libre accès à une installation 24 heures par jour, sept jours par semaine. L'accès est essentiellement réservé aux personnes qui ont affaire dans l'édifice pour les besoins du service et habituellement, l'accès 24 heures par jour, sept jours par semaine n'est accordé qu'à un occupant autorisé de l'édifice.

3. Systèmes de surveillance électronique d'accès. Au QGDN, on utilise à l'heure actuelle deux systèmes de surveillance électronique d'accès. Le système d'accès au périmètre principal est appelé Système intégré de contrôle d'accès (SICA). Un système secondaire appelé Système de contrôle de l'accès autonome (SCAA) sert à surveiller les allées et venues aux zones de sécurité internes de niveau supérieur. Le SMA(Fin SM) assure la gestion centralisée du SICA et l'USFC Ottawa, par le biais de la cie PM, en assure l'exploitation, alors que les systèmes SCAA sont exploités à l'appui de certaines organisations. Comme aucun de ces systèmes ne constitue à lui seul un obstacle suffisant à une entrée non autorisée, le personnel local ou de sécurité doit superviser les points d'accès. Les données recueillies au moyen des systèmes peuvent être utilisées dans le cadre d'enquêtes conformes à la loi, mais ne sont pas disponibles pour exercer un contrôle sur la présence au travail d'un employé ou d'un entrepreneur.

4. Cartes d'identité de la Défense nationale (NDI 20 et NDI 21). Ces cartes d'identité sont respectivement remises aux militaires et aux employés civils permanents des Forces canadiennes ou du ministère de la Défense nationale. Bien qu'elles ne soient pas conçues principalement pour servir de « laissez-passer », il est permis de les utiliser dans le SICA pour contrôler les allées et venues aux installations du MDN et des FC situées dans la RCN.

5. Laissez-passer/carte d'identité. Tous les membres du personnel doivent porter en tout temps le laissez-passer autorisé du QGDN placé à un endroit bien visible sur eux conformément à l'alinéa 5a), lorsqu'ils sont dans une installation d'accès contrôlé. Le laissez-passer du QGDN peut être remplacé par un laissez-passer spécial de secteur (à l'exception des cartes NDI 20/21 des militaires ou des employés civils permanents, car ce sont des cartes d'identité servant de « laissez-passer »). Il faut donc utiliser une deuxième pièce d'identité à photo conformément à l'alinéa 5c) ou à un point d'échange de laissez-passer à l'entrée dans une zone de haute sécurité (ZHS) du QGDN; il faut toutefois porter le laissez-passer du QGDN au sortir de la ZHS.

a. Le laissez-passer du QGDN ou la carte d'identité (selon le cas) se porte sur soi, à un endroit très visible entre la taille et l'épaule, la photo vers l'extérieur et les renseignements bien visibles. À la sortie d'un édifice du QGDN, le laissez-passer ne doit pas être porté en évidence, et doit être hors de vue.

b. Les laissez-passer spéciaux de secteur comme ceux qui servent à l'appui du Système de contrôle de l'accès autonome (SCAA) ne sont pas tenus pour des laissez-passer du QGDN et ne doivent pas être portés à l'extérieur du secteur d'accès réservé.

c. Sauf en ce qui concerne les détenteurs de cartes NDI 20/21 en vigueur, lesquelles sont reconnues à titre de cartes d'identité, les laissez-passer ne sont pas des cartes d'identité et à la demande de la police militaire ou du personnel de sécurité du QGDN, un détenteur de carte devra produire une deuxième pièce d'identité pour confirmer son identité et ses privilèges d'accès. Les pièces d'identité secondaires acceptables incluent le passeport, la carte d'identité du gouvernement fédéral ou toute autre preuve d'identité officielle fédérale ou provinciale.

d. Toutes les personnes à qui un laissez-passer du QGDN est délivré se voient aussi assigner un « numéro d'identification personnel » (NIP) par mesure de sécurité, pour compléter le balayage de la carte aux tourniquets du SICA. Cette mesure a pour objet d'empêcher une personne non autorisée de se servir d'une carte d'accès trouvée ou volée. Les cadres supérieurs de premier échelon (mais pas leurs subordonnés) peuvent dans la plupart des cas être exemptés des exigences relatives au NIP. Toutefois, si la sécurité l'exige, même les personnes habituellement exemptées d'utiliser un NIP peuvent être tenues de le faire.

e. La perte ou le vol d'une carte d'identité ou d'une carte d'accès doit être signalée sur-le-champ à la cie PM et au contrôle des laissez-passer, et le laissez-passer manquant sera désactivé dans le SICA. Il faudra présenter une demande/ autorisation de laissez-passer pour obtenir une carte de remplacement, et la direction/organisation d'appartenance peut se voir imposer les frais de remplacement (voir 7.04).

f. Les personnes qui oublient leur laissez-passer peuvent obtenir un « laissez-passer de visiteur sans escorte » pour la journée, moyennant une preuve de leur autorisation d'entrée. La preuve d'autorisation d'accès peut être vérifiée électroniquement, au moyen du SICA, ou si ce n'est pas possible, en faisant reconnaître la personne ou valider son identité par un collègue détenteur d'un laissez-passer en vigueur ou d'une NDI 20/21.

6. Privilèges d'accès. Les employés se verront accorder l'accès aux seules installations où ils sont censés avoir affaire. Habituellement, tout le personnel du MDN ou des FC employé au QGDN a l'autorisation d'avoir accès à l'édifice Mgén Pearkes et au lieu d'emploi normal pendant les heures de travail. S'il y a lieu, une personne peut aussi être autorisée à avoir accès à d'autres édifices pendant les heures de travail, et dans l'édifice où elle travaille pendant les

heures de fermeture. Sur demande de la police militaire ou du personnel de sécurité du QGDN, le détenteur d'un laissez-passer doit remettre le laissez-passer et quitter sur-le-champ le secteur d'accès contrôlé si on lui en donne l'ordre.

7.03 MESURES DE CONTRÔLE D'ACCÈS

1. Un garde supervise les points d'accès dans les principaux édifices du QGDN afin de contrôler les allées et venues et de mettre en application les règlements et les ordonnances en matière de sécurité. Dans certains édifices, on a installé un système interne de contrôle d'accès (SICA) électronique pour faciliter la tâche du personnel affecté au poste de garde. Toutes les personnes qui entrent dans des installations où le SICA est installé, ou qui en sortent, ont individuellement accès au système en soumettant leur carte à un balayage à l'entrée/sortie.

2. Les membres de la police militaire de l'USFC Ottawa ou du personnel de sécurité peuvent limiter ou restreindre les allées et venues dans un édifice en tenant compte de la menace sur place et ils sont tenus de remplir leurs tâches. Dans une situation de menace normale, l'accès est surveillé de près et les laissez-passer font l'objet d'un contrôle périodique pour en vérifier la validité, l'état et confirmer l'identité du détenteur. Quiconque refuse de se conformer aux demandes du personnel de contrôle d'accès ou de sécurité se verra refuser l'accès. Les personnes qui veulent sortir d'un secteur d'accès contrôlé avec de l'équipement appartenant au MDN ou aux FC ou des documents de nature délicate doivent avoir l'autorisation écrite d'apporter ces articles, conformément aux Directives en matière de sécurité de la capitale nationale 6.03, sans quoi on refusera qu'ils sortent avec le matériel.

3. Tout le personnel militaire ou civil a la responsabilité d'interroger les personnes qui ne portent pas de « carte d'identité » ou de « laissez-passer », pour s'assurer qu'elles ont l'autorisation d'entrer dans l'édifice ou les locaux de la direction ou de l'unité. Une personne qui ne possède pas de carte d'identité ou de laissez-passer en vigueur doit être escortée vers le point d'accès pour obtenir le laissez-passer approprié, ou doit quitter les lieux à la demande du personnel de sécurité.

4. Les personnes qui oublient leur laissez-passer peuvent obtenir un laissez-passer de visiteur en présentant une pièce d'identité pertinente et une preuve de leurs privilèges d'accès. Une personne qui ne peut être dûment identifiée et dont on ne peut vérifier l'autorisation d'accès se verra refuser l'accès au QGDN. Seul un détenteur de laissez-passer sans escorte peut servir d'escorte à une personne ayant besoin d'une escorte. Le personnel de sécurité doit consigner l'identité de l'escorte, et celui-ci est entièrement responsable du visiteur, et doit veiller à ce que la personne ayant besoin d'une escorte ne soit pas laissée seule ou sans surveillance.

7.04 OBTENTION ET COMPTABILISATION DES LAISSEZ-PASSER

1. Généralités. Sauf en ce qui concerne les NDI 20/21, tous les laissez-passer du QGDN appartiennent à l'USFC Ottawa et doivent être remis au moment d'une affectation ou d'une cessation d'emploi ou de contrat au QGDN. Les laissez-passer du QGDN et les NDI 20/21 sont des documents contrôlés remis à titre individuel, et les détenteurs ne doivent pas les échanger, les emprunter ni s'en servir pour permettre à du personnel non autorisé d'avoir accès aux installations. L'agent de sécurité de la direction ou l'agent de sécurité d'unité désigné qui autorise l'émission d'un laissez-passer a la responsabilité directe de veiller à ce que le détenteur soit mis au courant des directives et des protocoles sur la sécurité de la RCN et s'y conforme, et que le laissez-passer et la NDI 20/21 soient protégés comme il se doit.

2. Description et types de laissez-passer. Les laissez-passer du QGDN sont d'un modèle uniforme et présentent la photo, le nom et les données d'identification pertinentes du détenteur autorisé, ainsi que les privilèges d'accès à l'édifice et une date d'expiration. La couleur de la date d'expiration indique le niveau de sécurité du détenteur du laissez-passer : ROUGE – Niveau II ou autorisation de sécurité de niveau supérieur; VERT – Niveau I; BLEU – Vérification approfondie de la fiabilité; NOIR – pas d'autorisation de sécurité (il est à remarquer que la NDI 20 ou 21 ne contient pas cette information). Les divers laissez-passer du QGDN utilisés actuellement et les conditions d'admissibilité pour chaque type sont décrits ci-après :

a. Personnel du MDN:

1) Employés nommés pour une période indéterminée ou déterminée ou employés occasionnels du MDN;

2) Personnel particulier du ministre;

3) Employés des FNP/PSP;

4) Étudiants participant à un programme d'enseignement coopératif ou occupant un emploi d'été embauchés par le MDN ou les FC dans le cadre de programmes approuvés par l'État.

b. Membre de la Réserve des Forces canadiennes: Le personnel de la Force de réserve (Classe A, B, ou C) employé au QGDN (ou dans d'autres édifices confiés à la garde et au contrôle du commandant de l'USFC Ottawa).

c. Sécurité. Remis au personnel de sécurité de l'USFC Ottawa.

d. Visiteur accrédité. Les fonctionnaires d'autres ministères (c.-à-d. le Conseil du Trésor, TPSGC, etc.) et des sociétés ou organismes d'État qui sont employés au QGDN. Cette carte peut aussi être remise au personnel du :

1) Bureau de l'Ombudsman,

2) Comité d'examen des griefs des Forces canadiennes,

3) Commission d'examen des plaintes concernant la police militaire;

4) Forces alliées stationnées à Ottawa mais qui ne sont pas rattachées en permanence aux Forces canadiennes, et qui ont un besoin d'accès régulier et en vigueur.

e. Entrepreneur. Une personne employée par une entreprise ou un organisme engagé à contrat par le MDN ou les FC qui a besoin d'avoir accès aux installations du QGDN pendant une période déterminée.

f. Carte d'identité des Forces canadiennes et des civils. Bien que ces documents ne soient pas réellement des laissez-passer, il est permis d'utiliser la NDI 20 et la NDI 21 dans le SICA pour faciliter la surveillance électronique de l'accès. Les cartes d'identité du MDN et des FC sont des documents contrôlés délivrés conformément aux dispositions de la référence D.

g. Visiteur – Pas d'escorte nécessaire. Il est possible de délivrer un laissez-passer de visiteur à du personnel du MDN ou des FC qui visite le QGDN pour lui permettre d'avoir accès sans escorte à un édifice pendant les heures normales de travail. La présentation d'une carte d'identité de la Défense nationale ou l'identification formelle par une personne qui présente une carte d'identité en vigueur est une condition normale de libre accès. Moyennant une accréditation appropriée et une preuve d'autorisation de sécurité/vérification approfondie de la fiabilité, une personne qui n'appartient pas au Ministère peut obtenir ce laissez-passer quotidiennement et après une identification/vérification formelle de la part d'un agent autorisé du MDN ou des FC détenteur d'un laissez-passer sans escorte.

h. Visiteur – Escorte nécessaire. Les autres visiteurs seront escortés en tout temps et se verront remettre un laissez-passer qui précise cette condition d'accès.

i. Laissez-passer spécial de secteur/SCAA. Ce laissez-passer est délivré avec l'autorisation de la personne responsable du secteur d'accès spécial; des directives particulières doivent être respectées. Ces laissez-passer ne doivent pas se porter à l'extérieur du secteur d'accès spécial pour lequel le laissez-passer a été délivré.

3. Formule de demande de laissez-passer/accès. La formule DND 1102 (08-2000) servira à présenter une demande d'accès au QGDN. Les intéressés peuvent obtenir la formule auprès du contrôle des laissez-passer du QGDN ou sur le site RID de la cie PM (à l'adresse de l'USFC Ottawa).

4. Pouvoir de délivrer un laissez-passer. L'agent de sécurité de l'unité, du groupe, de la division ou de la direction peut accorder un laissez-passer au moyen d'une formule DND 1102 aux personnes admissibles du MDN ou des FC qui détiennent une autorisation de sécurité ou qui ont fait l'objet d'une vérification approfondie de la fiabilité; toutes les parties de la demande doivent être remplies. La demande d'une personne qui ne possède pas d'autorisation de sécurité ou qui n'a pas fait l'objet d'une vérification approfondie de la fiabilité sera recommandée par l'agent de sécurité responsable et approuvée par le commandant, le directeur général ou le directeur. Tous les intéressés doivent remplir la formule de demande/autorisation de laissez-passer (DND 1102), y compris ceux qui prévoient utiliser la NDI 20/21, car le document fournit la piste de vérification et l'information nécessaires pour activer la carte au moyen du SICA.

5. Durée de la carte. Les laissez-passer du QGDN ne seront délivrés que pour la période requise et en fonction de la durée de l'emploi. Aucun laissez-passer n'a une date d'expiration :

a. de plus de cinq ans à compter de la date d'émission;

b. en vigueur au-delà de la période d'emploi prévue;

c. ultérieure à celle de la carte d'identité d'employé du gouvernement du Canada.

6. Permis de visite – Industrie et autres ministères. Les visites au QGDN et aux établissements de la défense situés dans la RCN doivent être conformes aux protocoles d'autorisation du chapitre 40 des PEDN.

7. Laissez-passer perdu, volé ou endommagé. La police militaire et le contrôle des laissez-passer du QGDN doivent être avertis sur-le-champ de la perte ou du vol d'un laissez-passer afin que le personnel de sécurité puisse être alerté comme il se doit. Les laissez-passer endommagés rendus illisibles ou qui n'entrent plus dans le SICA seront remplacés le plus tôt possible. En cas de perte, de vol ou de dommages, l'agent de sécurité émetteur doit faire enquête sur les circonstances et fournir des renseignements détaillés au contrôle des laissez-passer du QGDN ainsi qu'une nouvelle formule d'autorisation de laissez-passer (DND 1102) et le code financier auquel un laissez-passer de remplacement peut être imputé. L'USFC Ottawa remboursera le remplacement seulement si la perte ou les dommages peuvent être directement attribués à l'unité (c.-à-d. un dommage normal attribuable au balayage dans le tourniquet du SICA relèverait de la responsabilité de l'USFC Ottawa). Les cartes d'identité doivent être signalées/remplacées conformément aux directives du Programme d'identification de la Défense nationale (PIDN).

8. Remise du laissez-passer à la cessation d'emploi et en cas de suspension. Les superviseurs et leurs agents de sécurité de soutien doivent veiller à ce que le laissez-passer d'un employé ou d'un entrepreneur suspendu ou quittant son emploi soit repris et remis au contrôle des laissez-passer du QGDN. Les personnes qui utilisent la carte NDI 20/21 pour avoir accès aux installations peuvent la conserver si elles continuent d'exercer leur emploi ailleurs au MDN ou dans les FC (conformément au PIDN), mais le contrôle des laissez-passer du QGDN en sera averti de manière à pouvoir mettre à jour le fichier du SICA.