National Défense
Defence nationale

Chef – Service d'examen

EXAMEN DE LA SÉCURITÉ DE L'INFORMATION AU MDN ET DANS LES FC

Octobre 2002

7050-7 (CS Ex)

Canada

TABLE DES MATIÈRES

SOMMAIRE

Le présent rapport fait la synthèse des résultats d'un examen concernant la sécurité de l'information au ministère de la Défense nationale (MDN) et dans les Forces canadiennes (FC). Fondé en grande partie sur des entrevues réalisées avec la collaboration d'une équipe de KPMG Consulting, l'examen comporte une évaluation des structures, des politiques et des pratiques organisationnelles du MDN et des FC relativement aux pratiques novatrices d'autres organismes en matière de sécurité de l'information. Le rapport a également mis à profit un examen parallèle de la conformité du Ministère à la Politique du gouvernement sur la sécurité (que l'on peut consulter sur le site Internet du CS Ex).

L'équipe d'examen a été témoin de l'évolution de la situation au sein du MDN et des FC et, à bien des égards, elle a pu documenter les points de vue des gestionnaires aussi bien que les initiatives prises en conséquence. (Elle a aussi élaboré une évaluation de référence sous forme de graphique en date de février 2001.) Parmi les principaux changements mis en œuvre vers la fin de l'examen, notons la création du Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC) et l'affectation du dossier de la gestion de l'information au Sous-ministre adjoint responsable de ce bureau. Cette mesure, ainsi que la création de la Direction – Sécurité (Gestion de l'information) (D Sécur GI) au sein du Groupe de la gestion de l'information, ont jeté les bases de structures à l'appui des recommandations de l'examen. La nécessité d'un point de contact en matière de sécurité de l'information est au nombre des recommandations principales de l'examen.

Naturellement, les politiques applicables à la sécurité de l'information reposent sur une tradition de rigueur policière. Parallèlement, les initiatives prises par les Opérations de sécurité ont fait évoluer les outils de contrôle et les techniques de surveillance de la sécurité de l'information. On note aussi que depuis l'examen, le MDN et les FC ont confié la responsabilité de la connectivité externe des systèmes à un Centre perfectionné d'essai et de développement.

Le plan d'action exhaustif de la direction, un élément clé du rapport, se trouve à l'annexe A. Parmi les nombreuses initiatives envisagées, mentionnons les suivantes : combler les postes de la Direction – Sécurité (Gestion de l'information), réviser le cadre de la politique en matière de sécurité de l'information et lancer un programme provisoire de sensibilisation.

Certes, le plan d'action de la direction visant à donner suite aux recommandations du présent rapport aura une incidence sur les ressources des organisations visées, ce dont il faudra tenir compte durant le processus habituel de planification des activités.

Cet examen a été effectué dans le cadre du plan de travail approuvé pour le Service d'examen. Les conclusions n'ont pas le poids de celles d'une vérification et ne doivent pas être perçues comme telles. L'examen permet de faire des recommandations à la direction, mais les évaluations et les conclusions qu'il renferme ne se fondent pas sur le type d'enquête rigoureuse et de preuves qu'une vérification exigerait. Les lecteurs du rapport doivent donc considérer les recommandations en conséquence.

APERÇU GÉNÉRAL

INTRODUCTION

1. Dans le cadre du plan d'examen 2000-2001, le Chef – Service d'examen (CS Ex) a évalué la pertinence, l'actualité et la fiabilité des pratiques du MDN et des FC en matière de sécurité de l'information, particulièrement du point de vue de la gestion des risques. Cet examen a été réalisé entre septembre 2000 et mars 2001.

2. L'examen avait pour but de fournir à la haute direction du Ministère des constatations, une analyse et des recommandations concernant la sécurité de l'information. L'examen comportait des recherches sur les pratiques novatrices adoptées par d'autres grandes organisations.

Évaluation comparative du Programme de sécurité de l'information au MDN et dans les FC

3. L'expérience du gouvernement américain. Le document *Learning From Leading Organizations,* publié en mai 1998 par le General Accounting Bureau (GAO) des États-Unis, porte notamment sur la gestion de la sécurité de l'information. On y examine les pratiques de huit grandes organisations non fédérales réputées pour la valeur de leurs programmes de sécurité de l'information. Cinq grandes pratiques se dégagent : reconnaître les ressources d'information comme des biens essentiels; élaborer des méthodes pratiques d'évaluation des risques; tenir responsables les gestionnaires des programmes et des activités; assurer une gestion continue des risques; et confier à un groupe central la réalisation d'activités clés comme l'élaboration des politiques connexes, la sensibilisation des utilisateurs et la surveillance des programmes. Même si le programme du MDN et des FC intègre déjà des éléments de chacune de ces pratiques novatrices, il a encore besoin d'améliorations.

4. Représentation graphique de l'évaluation. Comme en témoigne l'évaluation sommaire qui est présentée sous forme de tableau à la fin de cette section (page 5), les divers éléments du programme de sécurité de l'information au MDN et dans les FC peuvent aller de « non établi » à une « pratique évoluée ». L'examen a porté sur les sept composantes ci-après de la sécurité de l'information : 1) l'organisation de sécurité; 2) les politiques, les procédures et les lignes directrices connexes; 3) la formation et la sensibilisation en matière de sécurité; 4) la gestion des risques; 5) les opérations de sécurité; 6) la mise en œuvre de la sécurité et 7) les infrastructures essentielles. Il faudra se pencher sur des questions importantes comme l'orientation générale, les politiques sous-jacentes, de même que la formation et la sensibilisation. D'autres secteurs témoignent de l'exercice de bonnes pratiques de gestion.

5. Gestion des risques. En règle générale, les pratiques de gestion des risques en matière de sécurité de l'information s'améliorent, mais elles demeurent assujetties à la restriction des ressources et aux incessantes pressions opérationnelles qui s'exercent. Par ailleurs, le MDN et les FC sont sur le point de renoncer à l'approche basée sur des règles établies en faveur d'une approche axée sur les risques. Les responsables de la sécurité tâchent d'adapter les prescriptions de sécurité aux risques connus et d'augmenter la participation des cadres fonctionnels aux processus de gestion des risques et aux compromis nécessaires.

6. Point de contact de l'organisation. L'équipe d'examen a conclu que la principale source de préoccupation est la nécessité d'un bureau de première responsabilité (BPR) distinct chargé de la sécurité de l'information au Ministère, qui serait également responsable des politiques, de la formation, de la sensibilisation et de la surveillance connexes. Si d'autres organismes ont aussi éprouvé de la difficulté à cet égard, la plupart ont évolué, ou évoluent, dans le sens de l'approche de la Defense Information Systems Agency (DISA) et du ministère de la Défense des États-Unis (DoD). Selon cette méthode, la sécurité de l'information relève de la GI au niveau de l'organisation, tandis que la mise en œuvre du programme est de plus en plus déléguée aux gestionnaires opérationnels ou fonctionnels.

7. **NOTA :** Durant l'examen, à compter du 1er octobre 2001, le MDN et les FC ont établi un point de contact pour les questions relatives à la sécurité de l'information, soit la Direction – Sécurité (Gestion de l'information) (D Sécur GI), qui relève du Directeur général – Opérations (Gestion de l'information) (DGOGI) au sein du Groupe de gestion de l'information. En même temps, il a été reconnu que la sécurité de l'information n'est qu'un élément, si important soit-il, de la sécurité concernant le MDN et les FC. Les services de sécurité à l'échelle du Ministère devraient coordonner et intégrer plusieurs aspects, dont le personnel, le matériel, l'information et des considérations administratives/opérationnelles. Cela constitue un défi de taille pour le titulaire du poste d'agent de sécurité du Ministère (ASM), c'est-à-dire le Grand prévôt adjoint (Sécurité), qui relève du Grand prévôt des FC. Vu l'importance de cette fonction et des responsabilités connexes, il serait peut-être avantageux d'examiner le niveau hiérarchique et la visibilité de ce poste.

RECOMMANDATIONS

Les recommandations qui suivent découlent de notre examen et évaluation.

Établir un point de contact pour la sécurité de l'information

8. Le GAO a reconnu l'importance d'établir un point de contact pour la sécurité de l'information, chargé de coordonner des initiatives communes, d'évaluer les risques, d'établir et de tenir à jour des politiques et un plan central en matière de sécurité de l'information, de promouvoir la sensibilisation et de veiller à la sécurité de l'information. Ce point de contact peut aussi servir à optimiser l'affectation et l'emploi des ressources en matière de sécurité.

9. On a adopté cette pratique au MDN et dans les FC. Maintenant que le point de contact pour la sécurité de l'information a été établi (le D Sécur GI du Groupe de gestion de l'information), on peut procéder à la mise en œuvre des autres recommandations principales.

Officialiser et normaliser la création de politiques

10. Les politiques relatives à la sécurité de l'information ont besoin de beaucoup d'améliorations si l'on veut qu'elles soient efficaces. Les politiques connexes devraient inclure tous les aspects de l'information, les éléments manuels aussi bien qu'automatisés (autrement dit, le traitement et la technologie de l'information). Elles devraient être divisées en deux : des directives concises de haut niveau et des procédures plus détaillées. Il conviendrait que les politiques soient élaborées par le D Sécur GI et que les procédures relèvent de la responsabilité

des unités. Même si la distinction entre les politiques et les procédures se fait déjà dans certaines unités, la recommandation vise à officialiser et à normaliser ce processus et à le compléter par une fonction de surveillance incombant au D Sécur GI.

Élaborer un programme de formation et de sensibilisation

11. Le programme actuel de formation et de sensibilisation en matière de sécurité de l'information au MDN et dans les FC n'est ni structuré ni officiel. Il faut améliorer la formation offerte aux employés afin de réduire la probabilité et la gravité des incidents de sécurité ou des manquements à la sécurité. Négliger les questions de formation et de sensibilisation pourrait avoir pour effet de limiter l'exploitation des nouvelles technologies au sein du MDN et des FC. Il conviendrait que le D Sécur GI soit responsable de la coordination du programme. On devrait élaborer à cet égard des séances continues de sensibilisation à l'intention des cadres supérieurs.

Adopter un cadre de gestion des risques

12. Les changements importants touchant la connectivité attendue des systèmes d'information du Ministère ont sensiblement accru les menaces et les risques inhérents. Ce contexte technologique évolutif a aussi pour effet de changer la façon dont les organisations doivent gérer les risques. En ce qui touche la sécurité de l'information, celles-ci ne peuvent plus se permettre d'éviter les risques ou de se fonder sur des règles établies comme c'était le cas autrefois. Par exemple, plutôt que d'essayer de protéger tous ses renseignements, le MDN et les FC devraient tâcher de se concentrer sur les renseignements les plus indispensables. Comme le fait le DoD, 80 p. 100 des ressources accessibles pourraient servir à protéger les 20 p. 100 de renseignements qui sont les plus essentiels, tandis que le reste de l'information pourrait être échangée plus ouvertement. Il faut accepter des risques aux paliers inférieurs de l'organisation, afin de promouvoir la responsabilisation et afin qu'une telle stratégie donne des résultats. Cela exigera une plus grande régularisation et documentation de la gestion des risques, de manière à favoriser l'amélioration du cadre de gestion des risques.

Moderniser l'architecture de la sécurité de l'information

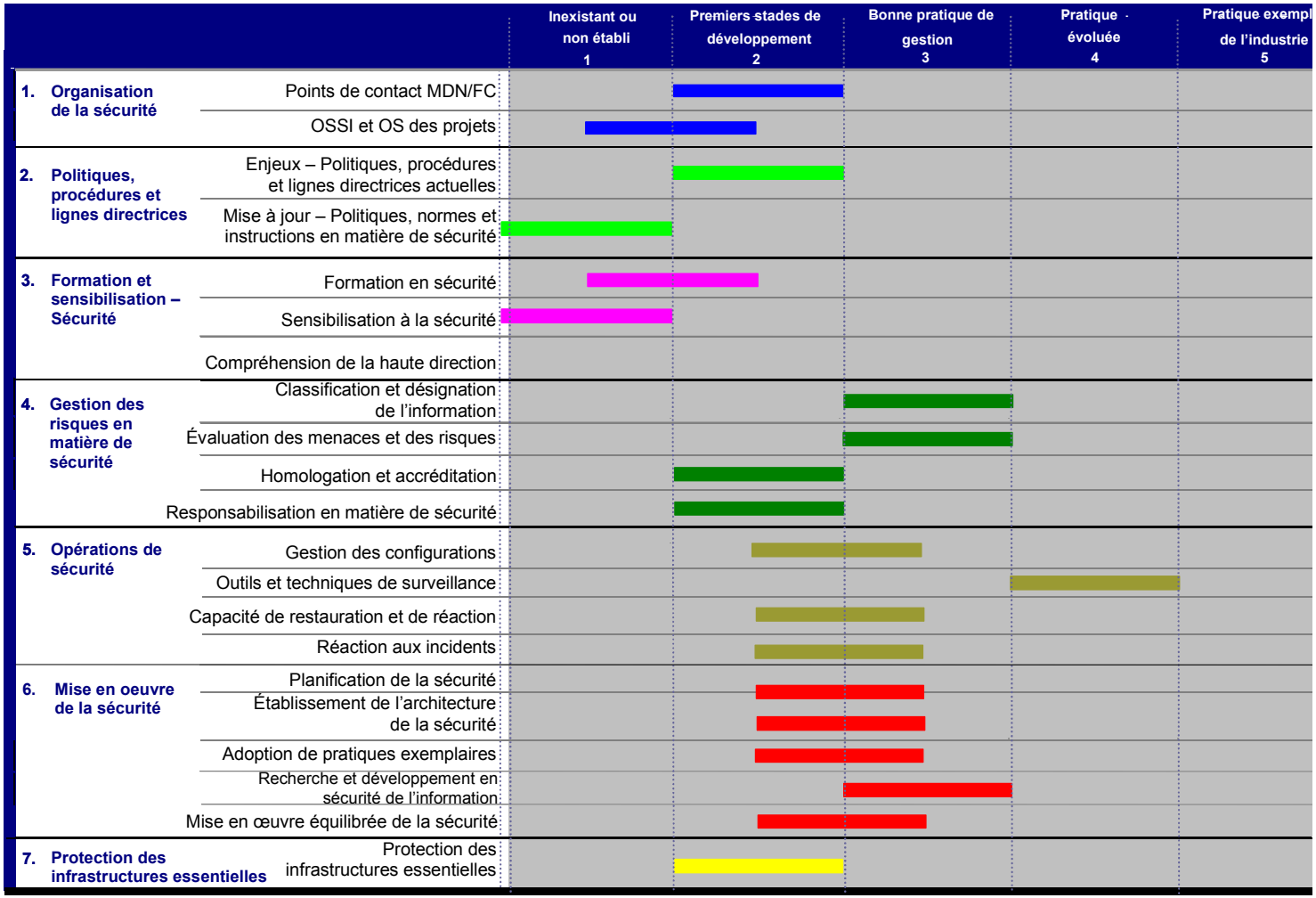
13. Les personnes du milieu de la TI que l'on a interrogées lors de l'examen (de 40 à 50 membres du personnel supérieur de la TI en septembre 2000) étaient toutes d'avis que l'architecture de sécurité de l'époque n'était pas à jour, quoique certaines d'entre elles savaient que l'on prenait des mesures afin de l'améliorer. On nous a fait comprendre que même si la nouvelle architecture de sécurité n'est pas encore officielle, elle est mise en œuvre. Il faudrait veiller à régulariser et à documenter cette nouvelle architecture de sécurité et à obtenir les approbations nécessaires.

Infrastructures essentielles

14. Un bon nombre des questions auxquelles se heurte le nouveau Bureau de la protection des infrastructures essentielles et de la protection civile (BPIEPC) se rapprochent de celles analysées dans le cadre de cet examen, à la différence qu'elles sont à plus grande échelle. Le rôle qui incombe au nouveau bureau est de servir de point de contact pour les travaux d'analyse et de coordination du gouvernement fédéral relativement aux incidents informatiques et d'aider

les ministères et organismes fédéraux à exercer leurs responsabilités en matière de sécurité. Par conséquent, les activités de la D Sécur GI devraient faire l'objet d'une étroite coordination avec celles du BPIEPC. Cette synchronisation des mesures de sécurité assurera une application uniforme des ressources restreintes et des pratiques novatrices, de même que l'amélioration continue des opérations de sécurité.

Gestion de la sécurité de l'information – Évaluation sommaire en date de février 2001



ANNEXE A

PLAN D'ACTION DE LA DIRECTION

Partie I – Organisation de la sécurité de l'information

1. Le SMA(GI), sous la responsabilité du DGOGI, a établi la Direction – Sécurité (Gestion de l'information) (D Sécur GI) à compter du 1er octobre 2001. Depuis octobre 2001, les effectifs de la D Sécur GI ont été confirmés et sont réunis en six sections :

a. D Sécur GI (Coordination) – planification des activités, bibliothèque de documents et soutien administratif;

b. D Sécur GI 2 – politiques relatives à la sécurité de la GI, formation et sensibilisation du personnel, homologation et accréditation des systèmes de GI, services de contrôle et de vérification;

c. D Sécur GI 3 – gestion de la sécurité du domaine désigné, y compris la gestion du service d'infrastructure à clés publiques (ICP) (matériel désigné);

d. D Sécur GI 4 – gestion de la sécurité du domaine classifié, dans lequel on distingue le matériel dont la cote peut aller de « Sans classification » à « Secret », d'une part, et le matériel portant la cote « Très secret » ou une cote supérieure, d'autre part, ainsi que la gestion du service ICP (matériel classifié);

e. D Sécur GI 5 – gestion du programme de sécurité de la GI, y compris les plans, les exigences et les normes (à l'échelle internationale et nationale) de sécurité applicables à la GI;

f. USCFC – soutien cryptographique du MDN et des FC, y compris la gestion du Système classifié canadien de gestion électronique des clés (SCCGEC).

2. Il reste de nombreux postes à combler, mais des mesures sont prises en parallèle afin de doter des postes civils de directeur, entre autres, et plusieurs postes professionnels de CS 02 INFOSEC au sein de la direction. Ces activités se poursuivent sans relâche depuis décembre 2001. Le DGOGI a indiqué que la D Sécur GI figure en tête de la liste des priorités pour ce qui est de la dotation en personnel en 2002-2003 et en 2003-2004. On s'attend que la transition de la D Sécur GI soit achevée et que 80 p. 100 des postes soient comblés d'ici **septembre 2003**.

ANNEXE A

Partie II – Politiques, procédures et lignes directrices – Sécurité de l'information

3. Le D Sécur GI et le GPA Sécur ont entamé une révision du cadre de la politique relatif à la sécurité de l'information. Ce cadre, y compris les pouvoirs, la structure de la documentation, la fréquence d'examen et les moyens de diffusion de l'information, est une première étape essentielle de l'amélioration des politiques relatives à la sécurité de l'information au MDN et dans les FC. Le GPA Sécur a accepté que le D Sécur GI soit chargé de la rédaction, de la révision et de la mise à jour des principaux chapitres des Instructions de sécurité de la Défense nationale (ISDN) concernant la sécurité de l'information (c.-à-d. les chapitres 70 et 71). Une nouvelle sous-section a d'ailleurs été établie au sein de la D Sécur GI pour s'occuper principalement des politiques, de la formation et de la sensibilisation. Cette tâche exigera un cycle continu d'examen, de révision, de publication et de diffusion au cours des **deux prochaines années** et dépendra des ressources qu'on y consacrera.

4. La D Sécur GI se trouve déjà sur l'intranet du MDN, de même que des liens vers d'autres sources et sites de renseignements sur la sécurité de l'information, mais il reste à établir des mesures d'unification et de rationalisation et à offrir en ligne une bonne collection de ressources documentaires. La structure du contenu du site Web de la D Sécur GI sera examinée de **septembre à décembre 2002** et un plan sera élaboré en vue de la modifier pour donner clairement accès aux politiques, ressources didactiques, procédures, lignes directrices, normes et instructions d'INFOSEC. Cela devra également se faire dans tous les domaines d'information (c.-à-d. pour les renseignements désignés et classifiés). On prévoit la mise en œuvre graduelle d'un portail Web sur la sécurité de l'information au cours de la période de **janvier à septembre 2003**, dans la mesure où les ressources le permettront.

Partie III – Formation et sensibilisation en matière de sécurité de l'information

5. La D Sécur GI, et autrefois le Centre de protection de l'information, a assumé la responsabilité de la formation et de la sensibilisation des professionnels de la sécurité de l'information et des membres des FC par le lancement et la soumission pour approbation d'un programme de sensibilisation, ainsi que d'une série de CQS et de DS. Ce travail d'état-major avance bien et les équipes du D Sécur GI et du SMA(RH-Mil) ont pris des mesures précises dans les deux cas, mais il s'agit d'une solution qui répondra aux besoins à plus long terme du MDN et des FC, **à compter de 2003-2004**.

6. Entre temps, la D Sécur GI étudie la mise en œuvre d'un programme provisoire de sensibilisation, basé sur ceux qu'ont adoptés d'autres ministères et des pays alliés, afin de combler la période d'ici à ce que le Ministère établisse un programme officiel de formation et de sensibilisation. Ces deux mesures seront menées de front, selon les ressources disponibles, et la priorité sera accordée au programme de formation et de sensibilisation à plus long terme. La coordination avec l'examen de structures de groupes professionnels connexes, comme le PARA, fera partie de ces mesures, tout comme la création et la validation de CQS, de DS et de plans de formation approfondis. Ces activités se poursuivent et l'on s'attend à la mise en place d'un programme de sensibilisation provisoire d'ici **novembre 2002**.

ANNEXE A

Partie IV – Gestion des risques de la sécurité de l'information

7. Le processus d'homologation et d'accréditation est reconnu comme encombrant et inutilement complexe pour la grande majorité des systèmes d'information. L'équipe de la D Sécur GI, de concert avec le système de gestion et les intervenants en sécurité de l'information, a examiné le processus en vigueur afin de rationaliser et de synchroniser les mécanismes existants de contrôle des configurations, telles les modalités de demande de changement relevant des Conseils nationaux de contrôle de la configuration de la GI depuis juillet 2001. La D Sécur GI entend pondérer les besoins d'homologation et d'accréditation en fonction de la valeur et la sensibilité des renseignements (et du système d'information) à accréditer. Cela s'apparente aux processus qu'emploie le ministère de la Défense des États-Unis. On vise également à utiliser le plus de documentation possible émanant d'autres processus (tels la documentation de projet, l'architecture des systèmes, le concept d'opération, etc.) afin de réduire les chevauchements. Le D Sécur GI a déjà modifié les documents définitifs d'accréditation en fonction d'une approche plus directe de gestion des risques, et ce par l'intégration des gestionnaires de systèmes et des responsables techniques de systèmes à la chaîne de responsabilisation avant l'acceptation définitive des risques par l'autorité compétente au niveau opérationnel. Dans un cas, les conditions d'accréditation d'un important système d'information tactique sont devenues des directives applicables à tout un commandement et à d'autres intervenants. La révision du processus d'homologation et d'accréditation se fera de manière continue, mais une première révision doit être achevée d'ici **décembre 2002** si les ressources le permettent.

8. Il est à noter que même s'il est recommandé dans le rapport du CS Ex d'accepter les risques à des paliers inférieurs de l'organisation pour encourager la responsabilisation, cela contraste avec la tendance à accroître de plus en plus l'interconnectivité des systèmes, d'où la tendance à courir des risques réels à des échelons de plus en plus élevés. Par exemple, il est peut-être logique que le commandant d'un déploiement opérationnel accepte les risques inhérents au fait d'avoir accès à un système national de commandement et de contrôle ou à un système de renseignement local, mais le risque réel qui se pose à ces fonds de renseignements ou systèmes d'information incombe à un niveau bien supérieur, en raison de la connectivité et de la facilité relative avec laquelle n'importe quel utilisateur (qu'il soit autorisé ou non) accède à un éventail de renseignements qui ne se limitent pas à ce théâtre opérationnel.

Partie V – Opérations de sécurité de l'information

9. La configuration des systèmes nationaux, qu'ils renferment des renseignements classifiés et désignés ou des données sans classification, relève des Conseils de contrôle de la configuration (CCC GI) connexes, sous la direction du DGOGI. Le D Sécur GI fait office de conseiller principal des CCC du matériel désigné et du matériel classifié. Cette activité exige énormément de ressources et de temps, et un bon nombre des outils qui permettraient de contrôler les configurations de manière plus dirigée ne sont pas encore en place. On a confié au DIIRI de la DGOGI la tâche de réviser les modalités des CCC.

ANNEXE A

10. Le D Sécur GI et le GOIFC ont élaboré, avec l'aide du groupe d'experts-conseils DMR, un processus détaillé de traitement des incidents relatifs à la sécurité des systèmes d'information (ISSIH) destiné à être appliqué à l'échelle nationale autant que locale. Ce processus intègre le Centre d'opérations de réseaux des Forces canadiennes (CORFC), que l'on a établi le 3 septembre 2002 à la SFC Leitrim en réunissant les équipes existantes de gestion de réseaux et de sécurité informatique. Les modalités de traitement des incidents ont fait l'objet d'une vaste diffusion au MDN et dans les FC.

11. Le D Sécur GI et le CORFC examineront les capacités et les procédures actuelles d'évaluation de la vulnérabilité des réseaux, afin que les systèmes qui posent le plus de risques ou qui sont les plus névralgiques soient évalués en priorité. Cette fonction exige un vaste éventail de ressources et de compétences.

Partie VI – Mise en œuvre de la sécurité des projets de TI

12. L'architecture de la sécurité informatique du MDN a été modifiée pour la dernière fois en août 2000, et elle n'a pas encore été adoptée ni promulguée officiellement. Même s'il demeure en grande partie pertinent et à jour, le document qui en fait état sera révisé en fonction des travaux accomplis depuis lors dans les domaines suivants : sécurité des systèmes sans fil, connectivité avec les entrepreneurs, séparation des infrastructures du matériel désigné et classifié, réseaux polyvalents (GPNet), réseaux « Très secret », sécurité des ordinateurs portatifs, nouvelles mesures de sécurité applicables à la couche réseau, déploiement de systèmes anti-intrusion, dispositifs sécuritaires, défense contre les programmes malveillants, entre autres. Le document qui en découlera sera soumis pour fins d'approbation et de promulgation par l'entremise de la D Sécur GI d'ici **septembre 2003**.

13. Outre l'orientation et la direction de projets concernant tous les aspects de la sécurité informatique, un certain nombre d'initiatives indépendantes se poursuivent en vue de la mise en œuvre de l'architecture de sécurité de la TI. On étudie la possibilité d'une capacité organisationnelle visant la protection contre des cyberattaques spécifiques et ciblées. Des acquisitions à cet effet sont d'ailleurs prévues en **2002-2003**. On accentue les besoins de sécurité nécessaires au raccordement de domaines de sécurité complets que l'on a gardés séparés jusqu'à présent pour des raisons de sécurité. D'ici **août 2003**, on dotera en effectifs une équipe de soutien anti-intrusion et un poste d'ingénieur auxiliaire afin d'assurer la mise en œuvre de solutions en la matière. Une politique a été élaborée pour que l'interconnexion des domaines de sécurité relève d'un organe central. On poursuivra la recherche de moyens de faire respecter la posture de sécurité et la configuration des postes de travail et serveurs du MDN, et une voie à suivre sera élaborée d'ici **août 2003**. Enfin, on veillera à l'élaboration et à la coordination de politiques générales de sécurité applicables à la mise en œuvre d'infrastructures communes, tels un système d'exploitation de réseau (SER) et des services d'annuaires électroniques, à mesure que les nouvelles technologies seront exploitées **au cours des prochaines années**. Une gamme d'initiatives plus restreintes visent également à combler les lacunes de l'infrastructure en place en matière de sécurité.

ANNEXE A

Autres mesures à prendre

14. Améliorer le soutien opérationnel de la sécurité des SI. La D Sécur GI veillera à préciser et à mettre en œuvre les structures de gestion et de soutien de la sécurité des SI, y compris les rôles, les responsabilités, la responsabilisation et les modalités de rapport à l'intention des OSSI, des gestionnaires de systèmes, etc. On s'attend que cela soit achevé d'ici **décembre 2002**.

15. Définir et favoriser des partenariats essentiels. La D Sécur GI établira et resserrera des liens essentiels avec le BPIEPC, le CST, le MAECI, le GPA Sécur, le BCP, l'OTAN, le CCEB et d'autres organismes au cours des six à dix-huit mois qui suivront **(août 2002 – janvier 2004)**.

16. Établir une capacité en matière de normes et d'exigences. La D Sécur GI constituera une capacité de normalisation et d'analyse à l'appui de projets en TI afin de définir les besoins en matière de sécurité. Cette mesure ne remplacera pas le plus vaste processus d'établissement des exigences de sécurité; elle vise plutôt à combler l'absence de normes de sécurité précises dans certains secteurs au moment de la mise en œuvre de projets informatiques. Cette capacité existe en partie, mais elle dépend énormément des attributions de ressources et sera assujettie à la définition des exigences entourant la modernisation cryptographique. On prévoit mettre en œuvre cette capacité d'ici **septembre 2003**.