Aperçu
de la vérification et de l'examen de la sécurité des technologies de l'information

Produit pour le compte de :	l'Office national de l'énergie 444, Septième Avenue S.-O. Calgary (Alberta) T2P 0X8
Produit par :	TRM Technologies Inc. 151, rue Slater Pièce 100 Ottawa (Ontario) K1P 5H3
Date :	15 janvier 2004
N^{o} de contrat :	84084030164

FICHE D'APPROBATION

Produit par : _____

M. Harrop B.Sc. en ingénierie, MBCS Date :
Conseiller principal, sécurité des TI

Revu par : _____

R. Moxley Date :
Directeur, sécurité des TI

Approuvé par : _____

E. F. Martin Date :

Président, TRM Technologies

Table des matières

Introduction

Selon la version révisée de la Politique du gouvernement sur la sécurité (PGS), qui est entrée en vigueur en février 2002, les ministères doivent élaborer et mettre en oeuvre un programme de sécurité ciblant les éléments suivants : administration, opérations, matériel, personnel et technologies de l'information (TI). Bien que la nouvelle politique sera appuyée par des normes de sécurité opérationnelles et techniques et comprendra des exigences de base en matière de sécurité (certaines d'entre elles sont toujours en cours d'élaboration), les ministères et organismes sont responsables de la mise en oeuvre détaillée de leur programme. De plus, ils doivent effectuer leurs propres évaluations des menaces et des risques pour déterminer la nécessité d'aller au-delà des mesures sécuritaires de base.

D'après la nouvelle politique, les ministères et organismes sont tenus de surveiller et d'examiner activement leur programme de sécurité. En vue d'en évaluer la conformité aux exigences de la nouvelle politique et de fournir une rétroaction sur l'efficacité de cette politique, les ministères doivent aussi rendre compte des résultats de leur évaluation ou vérification internes au Secrétariat du Conseil du Trésor.

L'Office national de l'énergie (l'ONÉ ou l'Office) a pris un certain nombre de mesures pour rehausser la sécurité des TI depuis l'examen de l'Équipe d'inspection et d'évaluation de la sécurité (ÉIÉS) de la GRC en 1997. Le projet de l'ONÉ a été soumis à un examen et à une vérification de la sécurité en vue d'en évaluer la conformité aux exigences de la PGS et des politiques l'ONÉ, et de déterminer l'efficacité de la mise en oeuvre des politiques et des normes connexes. Les résultats de l'évaluation permettront à l'ONÉ d'obtenir tous les renseignements nécessaires pour évaluer son degré de conformité aux exigences de la Politique sur la sécurité des technologies de l'information et à ses objectifs administratifs.

L'évaluation de la sécurité fait l'objet d'un rapport exhaustif qui a été présenté à l'ONÉ. Comme les résultats de la plupart des inspections de la sécurité renferment des renseignements de nature potentiellement délicate susceptibles d'être utilisés par des attaquants éventuels, il est d'usage de protéger le rapport de telles inspections en le marquant d'après les exigences de classification du gouvernement pour veiller à ce que seules les personnes possédant un « besoin de connaître » puissent y accéder. Fidèle à cette pratique, le rapport d'inspection de l'ONÉ a été désigné PROTÉGÉ dans son intégralité. Toutefois, comme l'ONÉ se fait un devoir, quand cela est possible, de verser au dossier public les résultats de ses vérifications, le présent aperçu, de nature non délicate, a été préparé dans le but de fournir des renseignements sur la nature de l'inspection et les méthodes utilisées pour satisfaire à l'exigence de rapport du Conseil du Trésor au sujet d'inspections de ce genre.

Résumé

Le présent mandat de vérification et d'examen de la sécurité a été exécuté pour le compte de l'ONÉ sous les auspices du Comité de vérification et d'évaluation en vue de satisfaire aux exigences de surveillance et de compte rendu du Secrétariat du Conseil du Trésor (SCT). En vertu de la PGS, les ministères et organismes doivent surveiller et évaluer activement l'efficacité de leurs programmes de sécurité et en faire rapport régulièrement au SCT. L'examen a été fait du 1er octobre au 15 décembre 2003.

Les TI jouent un rôle fondamental dans les opérations de l'ONÉ de sorte qu'il est essentiel de protéger efficacement les biens liés à ces technologies (y compris les données). Cependant, de nouvelles menaces à l'endroit des infrastructures d'information surgissent continuellement, et de nouveaux types d'attaques sont lancés avec une fréquence accrue. Une évaluation approfondie de la sécurité des TI de l'ONÉ, effectuée en 1997 par l'Équipe d'inspection et d'évaluation de la sécurité de la GRC (ÉIÉS), a révélé un certain nombre de lacunes. Depuis lors, des mesures ont été prises pour rehausser la sécurité des TI. Toutefois, la configuration de ces dernières, ainsi que les politiques et procédures internes, a beaucoup changé au cours des dernières années. Le présent rapport, fruit d'une évaluation indépendante approfondie, examine le degré de conformité de l'ONÉ aux exigences de la politique sur la sécurité des TI et la façon dont il s'acquitte de ses obligations administratives. Le rapport permettra aussi à l'ONÉ de cerner les secteurs qui demeurent potentiellement vulnérables et ceux qui lui offrent des occasions d'améliorer sa posture de sécurité. (Il importe de noter que l'examen a porté exclusivement sur l'application des méthodes et procédures requises par la PGS et les normes opérationnelles connexes. Les mesures de sécurité techniques particulières à l'Office n'ont pas été évaluées.)

Un certain nombre de techniques ont été employées pour faire l'inspection de la sécurité. Des listes de contrôle ont été créées afin d'examiner la concordance des critères de vérification utilisés par l'ONÉ avec ceux du guide du Secrétariat du Conseil du Trésor intitulé *Sécurité des technologies de l'information − guide de vérification* (Guide du Secrétariat du Conseil du Trésor) et d'évaluer la conformité de l'ONÉ à la PGS et aux normes opérationnelles y afférentes (c.-à-d. aux normes de sécurité relatives au matériel et aux technologies de l'information de même qu'à la norme portant sur l'organisation et l'administration de la sécurité), ainsi qu'aux politiques connexes (Politique sur l'autorisation et l'authentification électroniques, Politique d'utilisation des réseaux électroniques, Politique sur la gestion de l'information gouvernementale). En termes quantitatifs, 234 critères ont été examinés pour que leur concordance soit évaluée au regard des critères du Guide du Secrétariat du Conseil du Trésor, 57 exigences ont été passées en revue pour fin d'évaluation de la conformité à la PGS et 167 éléments ont été étudiés aux fins d'étude de la conformité aux politiques et normes opérationnelles connexes. Enfin, le mandat d'examen et de vérification de la sécurité a comporté une inspection des locaux et des interviews avec des membres du personnel. Les principales constatations sont exposées dans le corps du rapport, tandis que les constatations faites à partir des listes de vérification et du rapport d'inspection y sont jointes en annexe.

Outre de cerner les secteurs où l'ONÉ pourrait améliorer sa posture de sécurité, le rapport présente des recommandations visant à rehausser la sensibilisation en matière de sécurité, à améliorer la gestion de la sécurité et à favoriser une culture axée sur la sécurité à tous les paliers de l'ONÉ.

Le rapport souligne aussi que le maintien efficace de la sécurité est une tâche permanente et non une activité ponctuelle.

Enfin, il renferme un total de 34 recommandations qui, si elles sont adoptées, permettront à l'ONÉ d'améliorer sa posture de sécurité globale.

1. Aperçu du processus d'examen et de vérification de la sécurité à l'ONÉ

1.1 Contexte

En février 2002, le Secrétariat du Conseil du Trésor (SCT) a instauré une nouvelle Politique du gouvernement sur la sécurité (PGS). En vertu de cette politique, les ministères et organismes sont tenus d'élaborer et de mettre en oeuvre un programme ciblant tous les aspects de la sécurité, y compris la sécurité des technologies de l'information (TI). Outre d'établir la façon dont ils appliqueront la nouvelle politique, ils doivent surveiller et évaluer activement l'efficacité de leur propre programme de sécurité.

Le dernier examen exhaustif de la sécurité des TI à l'ONÉ a été réalisé par l'Équipe d'évaluation et d'inspection de la GRC (ÉIÉS) en 1997. Depuis lors, un certain nombre de mesures ont été prises pour rehausser la sécurité. La configuration des TI, ainsi que les politiques et procédures internes, ont aussi été modifiées à maintes occasions depuis 1997. De plus, le personnel de l'ONÉ est beaucoup plus sensibilisé à l'importance de sauvegarder l'information et les systèmes de TI de l'ONÉ.

En vue de satisfaire aux exigences de surveillance et d'examen, le Comité d'évaluation et de vérification de l'ONÉ a autorisé le présent mandat d'examen et de vérification de la sécurité des TI, qui a été exécuté du 1er octobre au 15 décembre 2003. Les résultats de cet examen indépendant permettra d'évaluer l'efficacité globale des procédures adoptées pour assurer la sécurité des TI et la conformité aux exigences de la PGS et autres politiques connexes. Outre d'exposer de manière indépendante et exhaustive le degré de conformité de l'ONÉ aux exigences de la politique sur la sécurité des TI et la façon dont il s'acquitte de ses obligations administratives, le rapport permettra à l'ONÉ de cerner les secteurs où la mise en oeuvre pourrait faire défaut et ceux qui lui offrent des occasions d'améliorer sa posture de sécurité.

1.2 Importance de protéger l'infrastructure d'information de l'ONÉ

À l'instar de la plupart des organismes privés ou d'État, l'Office national de l'énergie se fie beaucoup aux TI, particulièrement à ses infrastructures d'information, pour remplir le mandat qui lui a été conféré. Bien que l'Office se soit toujours soucié de la sécurité des TI, les progrès récents de la réseautique et de la prestation des services en ligne ont grandement contribué à augmenter les risques d'attaques provenant de l'extérieur. L'utilisation répandue d'Internet expose notamment les organismes à une grande variété d'attaques pirates (dont les vers et virus, dénis de service et attaques portant atteinte aux banques d'information) en plus d'accroître considérablement la fréquence des tentatives d'intrusions. En plus des attaques visant les réseaux, les nouvelles technologies (la technologie sans fil, les appareils portables de stockage de données, p. ex.) ont ouvert la porte à de nouveaux types d'attaques et ont contribué à amplifier la vulnérabilité de l'information.

L'ONÉ dépend énormément de ses réseaux et ressources de TI. En conséquence, il est devenu impératif de veiller à l'efficacité des mesures de sauvegarde. Les bris de la sécurité pourraient causer la dégradation, l'interruption, voire l'arrêt complet des activités de l'ONÉ.

Bien que les mesures de la sécurité des TI ciblent généralement les menaces provenant de l'extérieur, particulièrement celles qui peuvent être mises à exécution à distance par la voie du réseau, il ne faut pas oublier la possibilité de menaces à l'interne. Ces dernières peuvent résulter d'incidents, de défaillances du matériel ou de l'environnement informatique, ou être causées par des actes soit délibérés, soit involontaires de la part d'un employé de l'ONÉ ou d'un entrepreneur. Bien qu'il faille s'efforcer de protéger le périmètre des TI contre les intrusions non autorisées, il est tout aussi important de protéger l'ONÉ contre toutes les menaces possibles, y compris celles existant à l'intérieur de l'Office, grâce à l'application de mesures défensives et de mécanismes de restauration.

1.3 Vérification et examen de la sécurité à l'ONÉ

Le présent mandat de vérification et d'examen de la sécurité à l'ONÉ comprend une évaluation de la conformité aux politiques et normes opérationnelles du gouvernement du Canada (GC), ainsi qu'un examen de la sécurité des TI dans les environnements de niveau 1[1] (politique sur la sécurité) et de niveau 2 (normes opérationnelles) de l'ONÉ. La plupart des aspects de la sécurité de niveau 3 (normes techniques) ont été exclus de l'examen (à cet égard, la présente inspection diffère de celle menée antérieurement par la GRC, qui ciblait également les aspects de la sécurité de niveau 3). Le présent examen vise principalement à évaluer si les exigences de la PGS sont satisfaites, à déterminer si des procédures et des politiques appropriées en matière de sécurité ont été adoptées à l'ONÉ et, enfin, si ces dernières sont adéquates et sont appliquées. Les questions techniques et de configuration ne sont pas abordées en détail dans l'examen. Par exemple,

[1] Le document de référence 1.1 définit les documents de sécurité selon trois niveaux : niveau 1 − politique sur la sécurité, niveau 2 − normes opérationnelles et niveau 3 − normes techniques.

l'examen a pour but de vérifier si des mécanismes de protection sont utilisés à l'ONÉ (garde-barrière, logiciel de détection d'intrusion [IDS], p. ex.), mais non d'établir s'ils sont employés de manière adéquate ou s'ils ont été configurés correctement. De plus, l'examen n'a pas pour objet d'évaluer les menaces ou les risques, ou toute autre vulnérabilité particulière. Il vise strictement la sécurité des TI, de sorte que les autres éléments de la sécurité dont il est question dans la PGS (sécurité matérielle et sécurité des employés) ne sont abordés que dans la mesure où ils ont une incidence sur la sécurité des TI.

1.4 Méthode

Il existe une panoplie de guides sur les divers types d'inspection de la sécurité, mais aucune méthode agréée particulière[2]. Par conséquent, les inspections de la sécurité sont généralement réalisées selon des formules distinctes qui peuvent néanmoins comporter des similitudes. La méthode adoptée pour réaliser le présent mandat de vérification et d'examen comporte plusieurs étapes et s'appuie sur un certain nombre de documents d'orientation, notamment le Guide du Secrétariat du Conseil du Trésor et d'autres dont on trouvera la liste sous *Références* dans la section 3.

La présente inspection de sécurité repose sur les éléments qui suivent : politiques et documents en vigueur à l'ONÉ, interviews auprès de membres du personnel de l'ONÉ, inspection des locaux et de l'environnement de traitement de l'information de l'ONÉ, et vérification de la conformité à des exigences particulières de la PGS au moyen de listes de contrôle.

Le Guide du Secrétariat du Conseil du Trésor) (réf. 1.1), qui renferme une liste de contrôle, a servi de point de départ à l'examen. Il faut toutefois noter que la dernière mise à jour du Guide date de 1996 et ne reflète pas les changements apportés à la PGS, qui est entrée en vigueur en 2002. La liste de contrôle utilisée pour le présent examen a été établie à partir des critères énoncés dans le Guide de 1996 , mais comprend aussi de nouveaux éléments qui tiennent compte des modifications apportées à la politique et de la situation particulière de l'ONÉ. Des listes supplémentaires ont également été créées afin d'évaluer la conformité à la PGS, aux aspects de niveau 2 pertinents (normes opérationnelles et politiques) et à certain nombre de politiques connexes, y compris la Politique d'utilisation des réseaux électroniques et la Politique sur la gestion de l'information gouvernementale.

Les listes de contrôle annotées, jointes en annexe au rapport, constituent des documents d'archive faisant état des éléments examinés et de leur évaluation. Elles sont le fruit de l'examen des documents, des processus et de l'environnement de l'ONÉ en plus d'interviews de membres du personnel.

[2] Au sein du gouvernement fédéral, les évaluations des menaces et des risques s'appuient généralement sur les méthodes proposées par la CST ou la GRC, mais ces dernières sont souvent modifiées pour répondre aux besoins et aux structures des organisations évaluées.

L'examen des documents de l'ONÉ a permis d'établir jusqu'à quel point les exigences de la PGS avaient fait l'objet de mesures concrètes et d'évaluer la pertinence de leur contenu. Il a aussi permis de relever les lacunes dans les politiques et les procédures de l'ONÉ.

Des membres du personnel chargés spécifiquement de la sécurité, de l'élaboration des systèmes, de la gestion des dossiers et de la mise au point des applications, ainsi que des utilisateurs finals, ont répondu aux questions qu'ont suscitées l'examen des documents et l'inspection subséquente des locaux.

Les interviews avec des membres du personnel ont joué un rôle essentiel dans la présente évaluation, car elles ont permis à ceux et à celles qui sont directement touchés par les politiques et procédures en vigueur de présenter leurs points de vue sur l'efficacité des mesures de sécurité en place à l'ONÉ et de proposer des améliorations possibles.

Enfin, l'inspection matérielle des lieux a été effectuée.

Les listes de contrôle ont été remplies à l'aide des renseignements recueillis dans le cadre des procédés mentionnés ci-dessus. Afin d'assurer leur exactitude, les gestionnaires responsables et les spécialistes techniques ont été consultés lorsque certains points nécessitaient des éclaircissements. Les observations ont été compilées pendant toute la durée du mandat et sont incluses dans l'exposé des constatations du présent rapport. Ces dernières sont fondées sur tous les intrants cités plus haut. L'exposé des constatations est en grande partie structuré selon l'ordre des éléments compris dans les listes de contrôle. S'y ajoutent toutefois des points qui ne figuraient pas dans les listes, ces derniers ayant été mis au jour durant l'inspection. De plus, le rapport traite brièvement d'un certain nombre de nouvelles technologies qui ne sont pas encore abordées dans les politiques (technologies sans fil, programmes actif/mobile, appareils portables de stockage de données, p. ex.)

2. Constatations

Tel qu'il a été mentionné plus haut, le mandat de vérification et d'examen a comporté plusieurs étapes, notamment un premier examen effectué au moyen de la liste de contrôle établie à partir du Guide du Secrétariat du Conseil du Trésor, un second examen de la conformité aux exigences de la PGS et politiques connexes du Conseil du Trésor réalisé à l'aide d'autres listes de contrôle, et une inspection des locaux de l'ONÉ. Les listes annotées et le rapport d'inspection figurent aux annexes A, B et C du présent rapport. On trouvera dans ces documents les « données brutes » recueillies au moyen des questions posées. L'inspection et les interviews ont aussi permis de mettre au jour des renseignements pertinents supplémentaires qui dépassaient le cadre des questionnaires ou des questions préétablies sur la sécurité matérielle. Certains sont abordés dans le rapport d'inspection matérielle (annexe C), et d'autres, jugés pertinents, sont traités dans la section *Analyse* du présent rapport, dans laquelle on trouvera aussi une évaluation de l'incidence de toutes les constatations.

L'évaluation des constatations de l'inspection est divisée en trois sections. La première présente un résumé de la conformité globale de l'ONÉ aux exigences des politiques du gouvernement. Formulée en grande partie en termes quantitatifs, elle fournit une évaluation générale du degré de conformité de l'ONÉ aux exigences respectives des politiques. La deuxième traite brièvement des constatations de l'examen effectué au moyen de la liste de contrôle du Guide de vérification de la sécurité. La dernière, la plus importante, présente une analyse des constatations issues de toutes les listes de contrôle et de l'inspection matérielle ainsi que des renseignements mis au jour durant l'examen. Cette section est en grande partie structurée selon l'ordre des éléments compris dans la liste de contrôle.

2.1 Conformité aux exigences des politiques

Selon la hiérarchie des politiques et normes opérationnelles du gouvernement en matière de sécurité, la PGS est située au sommet de la pyramide (niveau 1), les normes opérationnelles (comme celles qui portent sur la sécurité matérielle, la sécurité des TI et la sécurité du personnel) suivent immédiatement après (niveau 2) et les normes techniques (telles que les normes de sécurité techniques dans le domaine de la technologie de l'information [NSTTI]) se trouvent au troisième niveau. Cette hiérarchie est illustrée à la figure 1. Le présent examen a porté sur la vérification de la conformité aux exigences de la PGS, aux normes applicables de niveau 2 et aux exigences des politiques connexes en matière de sécurité des TI.

Les constatations au sujet de la conformité aux exigences des politiques font l'objet d'un résumé formulé principalement en termes quantitatifs. Bien qu'un tel résumé fournisse généralement une idée générale du respect des exigences, particulièrement en ce qui concerne les secteurs où la conformité à la politique est la plus faible, de telles données quantitatives doivent être interprétées avec prudence parce qu'elles ne donnent aucune indication de l'importance relative des secteurs jugés non conformes. Par exemple, le non-respect des exigences dans un secteur que l'ONÉ juge de faible priorité en ce moment occuperait vraisemblablement un rang très inférieur dans l'échelle de risque, mais, dans d'autres secteurs, cela pourrait révéler un risque sérieux. La section du rapport portant sur l'analyse traite de l'importance de la non-conformité.

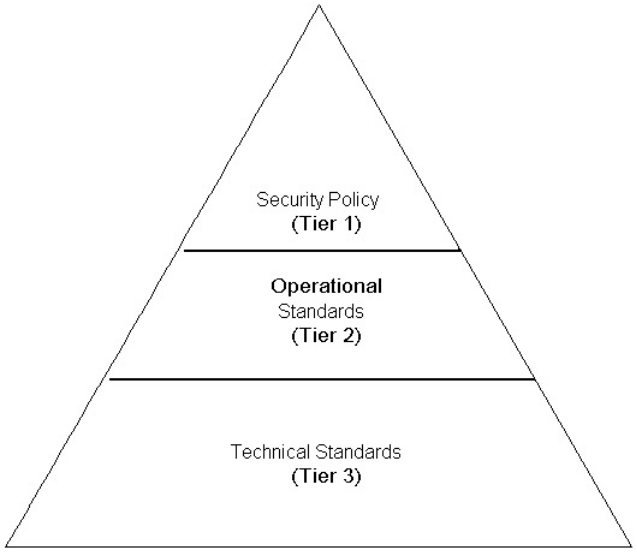

Figure 1 : Hiérarchie des documents de sécurité du gouvernement

2.2 Conformité aux exigences de la Politique du gouvernement sur la sécurité

Cinquante-sept exigences particulières ont été examinées pour évaluer la conformité globale de l'ONÉ à cette politique.

2.3 Conformité aux normes opérationnelles

Le mandat a porté sur l'évaluation de 13 exigences de la norme de sécurité matérielle, 55 exigences de la norme de sécurité des TI et 56 exigences de la norme relative à l'organisation et à l'administration.

2.4 Conformité aux exigences des politiques connexes

Les exigences pertinentes de la Politique sur l'autorisation et l'authentification électroniques, de la Politique d'utilisation des réseaux électroniques et de la Politique sur la gestion de l'information gouvernementale ont été examinées pour fins d'évaluation de leur degré de conformité.

2.5 Concordance avec les critères énoncés dans le *Guide de vérification de la sécurité*

La liste de contrôle du Guide du Secrétariat du Conseil du Trésor n'a pas été conçue pour vérifier la conformité à des politiques particulières, ou à d'autres exigences. Elle fournit uniquement un cadre pour évaluer si certaines pratiques exemplaires reconnues, formulées dans le Guide, ont été adoptées. Si tel n'est pas le cas, elle permet d'établir si les pratiques ayant cours sont équivalentes ou représentent une alternative suffisante. La liste de contrôle vise également à mettre les lacunes en relief. Toutefois, contrairement aux exigences de conformité aux politiques, nul n'est explicitement tenu d'adopter les critères de la liste de contrôle. De plus, les organismes dont certains critères ne concordent pas avec ceux de la liste de contrôle ne sont pas nécessairement perçus comme usant de mauvaises méthodes. Il est parfois possible de satisfaire à l'esprit des critères d'une toute autre manière que celle préconisée par ceux qui figurent dans la liste.

En termes quantitatifs, 234 critères de la liste de contrôle ont été examinés. Les écarts constatés durant la vérification sont expliqués dans les commentaires figurant dans la colonne des observations.

Les secteurs problématiques mis au jour dans la liste de contrôle correspondent dans une large mesure aux problèmes auxquels la politique fait allusion ou qui ont été mis au jour lors des inspections. On trouvera plus de détails à ce sujet, ainsi qu'un examen de leur incidence, dans la section *Analyse* du présent rapport.

2.6 Analyse des principales constatations de l'inspection

La section du rapport consacrée à l'analyse examine les principales constatations issues de l'inspection. Elle est en grande partie structurée selon les éléments compris dans la liste de contrôle et comporte les mêmes rubriques. Cependant, l'ensemble des constatations de l'inspection y est analysé, y compris les éléments qui ne figurent pas dans les listes de contrôle.

Les analyses et les constatations sont résumées sous les rubriques suivantes :

- Organisation et administration
- État du processus de planification de la sécurité des TI (STI)
- Liens fonctionnels
- Politiques, méthodes et procédures de l'Office en matière de STI
- Pertinence de la capacité, des méthodes et des procédures de gestion des risques pour la STI
- Pertinence des informations utilisées pour appuyer les décisions relatives aux risques
- Utilisation du cadre de gestion des risques de la STI approuvé par l'Office pour l'élaboration des TI
- Processus de gestion des risques de la STI pour maintenir à jour les TI opérationnelles
- Procédures de l'Office pour contrôler l'autorisation et l'accès aux systèmes liés aux TI
- Politiques, méthodes et procédures pour assurer la gestion, la réparation, la mise à jour et la destruction appropriées du matériel de STI
- Le personnel est conscient des politiques, méthodes et procédures de réparation et de mise à jour de l'Office et les respecte
- Vérifications internes de la STI
- Évaluations des menaces et des risques pour la sécurité des TI de l'Office
- La CST examine périodiquement les procédures de sécurité des communications et des systèmes de télécommunications de l'Office
- Contrats comportant des exigences relatives à la STI
- Examens de la STI, autoévalutations et examens internes de la sécurité
- Documents sur les énoncés de la nature délicate et sur les modes de fonctionnement des systèmes, des réseaux et des applications
- L'Office fait une enquête de sécurité avant de donner accès à des systèmes, des réseaux ou des applications qui traitent de l'information de nature délicate aux membres de son personnel
- Révocation des droits d'accès
- Programmes de formation et de sensibilisation à la STI − offerts à tout le personnel, y compris tous les utilisateurs et les gestionnaires
- Exigences matérielles et environnementales
- Politiques, méthodes et procédures relatives à la sécurité du matériel des TI et à la gestion de la configuration

- Contrôle de l'accès au télédiagnostic du matériel
- Politiques, méthodes et procédures régissant l'utilisation des logiciels privilégiés et puissants
- Politiques, méthodes et procédures relatives à la sécurité des communications et exigences relatives à la sécurité des communications dans les projets d'élaboration des TI
- Politiques, méthodes et procédures relatives à la sécurité des réseaux
- Les réseaux et applications réseaux des TI font l'objet de mesures de protection adéquates
- Politiques et procédures relatives à l'exploitation de la STI
- Informations partagées
- Responsabilités du personnel / problèmes de confiance
- Préoccupations relatives à la confidentialité électronique
- Classification des renseignements
- Accès à l'ordinateur serveur
- Surveillance des événements liés à la sécurité
- Télétravail
- Accès à distance
- Nouvelles menaces et technologies en évolution
- Normes d'interopérabilité
- Gestion de la banque d'informations

3. Conclusions et recommandations

En fonction des constatations du rapport, ce dernier comporte huit conclusions particulières assorties de 15 recommandations. De plus, 19 recommandations additionnelles résultent directement des constatations du rapport.

Acronymes et abréviations

GC	Gouvernement du Canada
PGS	Politique du gouvernement sur la sécurité
ISO	Organisation internationale de normalisation
TI	Technologie de l'inforamtion
STI	Sécurité des technologies de l'information
RCN	Région de la capitale nationale
ONÉ	Office national de l'énergie
OP	Ordinateur personnel
EIES	Équipe d'inspection et d'évaluation de la sécurité (GRC)
SCT	Secrétariat du Conseil du Trésor
EMR	Évaluation des menaces et des risques
RPV	Réseau privé virtuel
WAN	Réseau longue portée

Références

L'évaluation de la sécurité s'est appuyée sur les documents de référence ci-dessous.

1. Politiques, méthodes et procédures du gouvernement du Canada et du Conseil du Trésor

1.1 Sécurité des technologies de l'information − Guide de vérification, SCT, 1996
1.2 Politique sur la sécurité, SCT, février 2002
1.3 Politique sur l'autorisation et l'authentification électroniques, SCT, juillet 1996
1.4 Norme de sécurité technique dans le domaine de la technologie de l'information (NSTTI), GRC, août 1997
1.5 Politique sur la gestion de l'information gouvernementale, SCT, mai 2003
1.6 Norme sur la sécurité matérielle, Guide des politiques du SCT, ch. 2.2 (non daté)
1.7 Norme sur la sécurité du personnel, Guide des politiques du SCT,ch. 2.4, décembre 1993
1.8 Norme de sécurité relative aux technologies de l'information, Guide des politiques du SCT, juin 1995
1.9 Norme de sécurité et des mesures d'urgence, Guide des politiques du SCT, ch. 2.6 (non daté)
1.10 Politique d'utilisation des réseaux électroniques, SCT, février 1998
1.11 Norme de sécurité relative à l'organisation et l'administration, Guide des politiques du SCT, ch. 2.1, juin 1995
1.12 Politique de télétravail, SCT, décembre 1999
1.13 Guide d'utilisation, Système central de rapports de gestion financière, TPSGC, juin 2001

2. Politiques, méthodes et procédures de l'ONÉ

2.1 Politique et procédures de sécurité, ONÉ, juillet 2001
2.2 Organigramme du Comité de sécurité, juin 2003
2.3 Structure organisationnelle de l'ONÉ, juillet 2003
2.4 Évaluation globale de l'ONÉ, ÉIÉS, juillet 1997
2.5 Sécurité − Politique sur l'utilisation des services informatiques, juillet 1999
2.6 Utilisation des services informatiques − Questions et réponses (non datées)
2.7 Politique et procédures de la gestion des biens, mars 2002
2.8 Politiques et procédures d'accès à l'immeuble, novembre 2000 (Building Access Policies and Procedures, Nov. 2000)
2.9 Contracting of Temporary Help Policy and Procedures, février 2001
2.10 Contracting and Procurement Guide, mai 2002
2.11 Telecommunications Policy and Procedures, mars 2001
2.12 NEB Information Systems Methodology V2.0, septembre 2002
2.13 Configuration Management, Release Management & Change Management Combined Function, ébauche, 20 octobre 2003

2.14 Sécurité des renseignements consignés, chap. 10 et 11, manuel de gestion de la sécurité de l'ONÉ, février 1988.
2.15 Lignes directrices sur le traitement des renseignements de nature délicate, non daté et anonyme.
2.16 Rapport sur l'évaluation des menaces et des risques, ONÉ, décembre 1996.
2.17 Guide d'utilisation, Système central de rapports de gestion financière, sect. 3.2, octobre 2002

3. Autres documents de référence

3.1 Management Planning Guide for Systems Security Auditing, National State Auditors and US General Accounting Office, décembre 2001
3.2 Site Security Audit Checklist, G Halprin, SysAdmin Group, juin 2003
3.3 Computer Security Audit Checklist, C.Rose, ITSecurity.com, avril 2002
3.4 Data Centre Physical Security Checklist, Sean Hearn, Sans Institute, décembre 2001
3.5 Computer Security Audit Checklist, Chris Hardie, Summersault.com, avril 2003
3.6 Guidelines on Active Content and Mobile Code, Wayne Janson, NIST Special Publication 800-28, octobre 2001

Glossaire

Programme actif	Programme qui peut être transféré d'un réseau à un système local sans que l'utilisateur ait à effectuer des opérations explicites d'installation ou d'exécution.
Disponibilité	Propriété d'être accessible et utilisable à la demande par une entité autorisée (ISO 7498-2).
Contrôles de base	Ensemble minimum de mesures de protection établies pour un système ou un organisme.
Exigences de base en matière de sécurité	Dispositions obligatoires de la Politique du gouvernement sur la sécurité, des normes opérationnelles connexes et de la documentation technique
Confidentialité	Propriété des données qui indique qu'elles n'ont pas été rendues accessibles ou divulguées à des personnes, des entités ou des processus non autorisés. (IS 7498-2)
Intégrité des données	Propriété des données qui indique qu'elles n'ont pas été modifiées ou détruites d'une manière non autorisée (ISO 7498-2).
Garde-barrière	Passerelle d'interréseau créant entre deux réseaux une frontière qui sert à isoler, à filtrer et à protéger les ressources des systèmes locaux de la connectivité externe, par le contrôle du volume et du type de trafic autorisé à passer d'un réseau à l'autre.
Intégrité	Voir Intégrité des données.
Zone de sécurité TI	Environnement de réseau caractérisé par une frontière bien définie, une autorité de sécurité et un niveau normalisé de susceptibilité aux menaces pesant sur le réseau. Les différents types de zones de sécurité TI se distinguent par les mesures de sécurité prises à leurs interfaces, le contrôle du trafic, la protection des données, le contrôle de la configuration de l'hôte et le contrôle de la configuration du réseau.
Programme malveillant	Programme écrit intentionnellement pour effectuer des opérations gênantes ou nuisibles dans un ordinateur. Ils sont souvent travestis en programmes utiles ou incorporés dans des programmes utiles, de façon à être activés par une action de l'utilisateur. Les principaux types de programmes malveillants sont les chevaux de Troie, les virus et les vers.
Programme mobile	Programme qu'un scénario, une macro-instruction ou autre instruction portable qui peut être expédié à un ensemble hétérogène de plate-formes et être exécuté selon la même sémantique.
Vérification de sécurité	Revue et examen indépendants des enregistrements et des activités d'un système pour vérifier l'efficacité des contrôles du système, pour assurer la conformité aux politiques établies et aux procédures opérationnelles, pour détecter les atteintes à la sécurité et pour recommander les modifications qui s'imposent aux contrôles, aux politiques et aux procédures (ISO 7498-2).
Réseau privé virtuel sécurisé	Réseau privé virtuel (RPV) utilisant une technique de cryptographie (par exemple, IPsec) contrairement aux réseaux privés virtuels dont la sécurité est simplement fondée sur l'isolement logique (par

(RPVS)	exemple, MPLS ou VLAN Ethernet).
Menace	Violation potentielle de la sécurité (ISO 7498-2).
Réseau privé virtuel	Réseau informatique à usage restreint, réalisé par logique, (c'est-à-dire par moyens artificiels ou de simulation) construit à partir des ressources d'un réseau physique (c'est-à-dire réel) relativement public (comme Internet), souvent avec chiffrement des données (au niveau des hôtes ou des passerelles) et souvent avec des tunnels du réseau virtuel établis à travers le réseau réel.