Travaux publics et Services gouvernementaux Canada
Public Works and Government Services Canada
Canada

Rapport final

2009-713
Vérification des renseignements classifiés traités par voie électronique

Le 10 mai 2012

Bureau de la vérification et de l'évaluation

www.tpsgc-pwgsc.gc.ca

TABLE DES MATIÈRES

POINTS SAILLANTS

Objet

i. L'information ou renseignements de nature délicate est l'information qui doit être protégée, car sa divulgation, son altération, sa perte ou sa destruction pourrait porter préjudice à des biens ou à des personnes. Il existe deux types d'information de nature délicate au gouvernement du Canada : les renseignements protégés et les renseignements classifiés. Les renseignements protégés sont les renseignements n'étant pas d'intérêt national. Les catégories de protection sont les suivantes : Protégé A, Protégé B et Protégé C. Les renseignements classifiés correspondent à l'information de nature délicate dont la divulgation non autorisée risquerait vraisemblablement de porter préjudice à l'intérêt national, c'est-à-dire à la sécurité et à la stabilité sociale, politique et économique du Canada. Les catégories de classification sont, par ordre croissant de sensibilité : Confidentiel, Secret et Très secret. Le traitement des renseignements électroniques classifiés comprend entre autres la création, l'entreposage, la transmission et la destruction des renseignements classifiés.

ii. Une série d'instruments de politique publiés par le Bureau du Conseil privé, le Secrétariat du Conseil du Trésor, les organismes responsables de la sécurité, comme la Gendarmerie royale du Canada, et Travaux publics et Services gouvernementaux Canada (TPSGC) contiennent les exigences à respecter pour protéger les renseignements classifiés traités par voie électronique au sein du Ministère.

iii. Cette vérification visait à examiner la conformité de trois directions de la Direction générale des services ministériels et des politiques stratégiques (DGSMPS) à certaines exigences des instruments de politique pertinents. Ces directions traitent des renseignements classifiés par voie électronique dans le cadre de la prestation des services au Ministère.

iv. La Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC) ainsi que la Direction des affaires relatives au Conseil du Trésor (DACT) fournissent aux agents de TPSGC un centre d'expertise pour les aider à créer les documents du Cabinet et les présentations au Conseil du Trésor qui ont trait aux initiatives de TPSGC. La troisième direction, la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP), administre la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* au nom du Ministère.

v. Depuis le 15 novembre 2011, la sous-ministre adjointe de la Direction générale de la surveillance est chargée d'administrer le Programme de sécurité du Ministère. La Direction générale des services d'infotechnologie a la responsabilité générale du Programme de sécurité de la technologie de l'information (TI) du Ministère. La sous-ministre adjointe de la Direction générale des services ministériels et des politiques stratégiques est responsable d'élaborer un cadre de gestion des biens de TI et de gérer l'élimination des biens de TI conformément à ce cadre.

Pertinence

vi. Il est important de respecter les divers instruments de politique liés à la protection des renseignements classifiés traités par voie électronique, car cela réduit le risque que des personnes non autorisées accèdent à des renseignements classifiés confiés à TPSGC ou créés par ce dernier.

vii. Un accès non autorisé aux renseignements électroniques classifiés pourrait porter préjudice au Ministère, à ses clients et au gouvernement. De plus, cet accès non autorisé pourrait nuire à la confiance de la population canadienne envers le gouvernement du Canada.

Constatations

viii. Nous avons constaté que le traitement des renseignements électroniques classifiés n'était pas toujours conforme aux exigences des instruments de politique.

ix. Le réseau informatique de TPSGC était parfois utilisé pour la communication de renseignements classifiés jusqu'au niveau « Secret ». Ce réseau n'est pas destiné aux renseignements classifiés, mais seulement aux renseignements « Protégé B » encodés et aux renseignements « Protégé A » ou de nature moins délicate.

x. La Direction de l'AIPRP et la DPSAC traitaient des renseignements électroniques classifiés dans des systèmes de TI classifiés. Toutefois, le système de TI classifié utilisé par la DPSAC n'était pas toujours disponible au moment voulu, de ce fait, certains de ses membres ont traité des renseignements électroniques classifiés sur le réseau de TPSGC. La DACT n'avait pas accès à un système de TI classifié et, en conséquence, ses membres utilisaient le réseau de TPSGC pour traiter des renseignements électroniques classifiés.

xi. Même si les deux systèmes de TI utilisés par la DPSAC et la Direction de l'AIPRP pour traiter des renseignements électroniques classifiés avaient été certifiés pour traiter le niveau pertinent de renseignements de nature délicate, leurs certifications étaient périmées. Seul le système de TI classifié de la Direction de l'AIPRP avait été accrédité, et cette accréditation avait également pris fin. Le système de TI classifié de la DPSAC avait des identificateurs d'utilisateur actifs pour des personnes qui avaient quitté l'organisation, et les deux systèmes de TI utilisaient des identificateurs d'utilisateur génériques.

xii. Les personnes identifiées comme ayant accès aux systèmes de TI classifiés avaient une autorisation de sécurité adéquate. Il a toutefois été impossible de déterminer qui avait accès à certains identificateurs d'utilisateur génériques. Il a donc été impossible de déterminer si les personnes qui avaient accès à ces identificateurs d'utilisateur génériques possédaient toutes l'autorisation de sécurité requise. Les trois directions sélectionnées pour la vérification traitaient des renseignements électroniques classifiés dans des zones de sécurité matérielle appropriées.

xiii. De plus, les renseignements électroniques classifiés créés par les directions étaient marqués de façon appropriée, mais le matériel électronique utilisé pour traiter ces renseignements n'était pas marqué de façon systématique.

xiv. Enfin, aucun processus formel n'était place pour éliminer le matériel électronique classifié inutilisé.

Réponse de la gestion

La direction reconnaît que les constatations du rapport sont justes et exactes en ce qui concerne la façon dont les renseignements électroniques classifiés ont été traités par les trois directions visées par la vérification.

La direction donnera suite aux recommandations contenues dans le rapport de vérification en mettant en place le Plan d'action de la gestion suivant.

Recommandations et Plan d'action de la gestion

Recommandation 1 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce que les renseignements électroniques classifiés de la DGSMPS soient créés, entreposés et transmis uniquement dans des systèmes de TI adéquats, et que ces systèmes restent certifiés et accrédités au niveau approprié.

> **Plan d'action de la gestion 1.1 :** La Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC), la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et la Direction des affaires relatives au Conseil du Trésor (DACT) élaboreront et mettront en place des procédures internes liées à la création, à l'entreposage et à la transmission des renseignements électroniques classifiés, y compris des procédures de traitement des renseignements classifiés, si les systèmes classifiés de TI ne sont pas disponibles.
>
> Cette mesure sera mise en œuvre à la DPSAC au plus tard le 31 mai 2012, à la Direction de l'AIPRP au plus tard le 31 juillet 2012, et à la DACT au plus tard le 31 décembre 2012.
>
> **Plan d'action de la gestion 1.2.1 :** En tant que propriétaire de système d'affaires, la DGSMPS, en collaboration avec le coordonnateur de la sécurité de la TI, élaborera un plan de certification afin de faire accréditer les systèmes désignés ainsi que l'infrastructure connexe.

Plan d'action de la gestion 1.2.2 : Fournir au coordonnateur de la sécurité de la TI les éléments de preuve requis, tel que décrit dans le plan de certification, afin d'appuyer la réalisation du processus de certification et d'accréditation.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 28 septembre 2012, et à la Direction de l'AIPRP d'ici le 29 juin 2012.

Plan d'action de la gestion 1.2.3 : La DGSMPS signera la lettre d'accréditation soumise par le coordonnateur de la sécurité de la TI afin d'accepter les recommandations relatives au traitement des risques résiduels.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 30 novembre 2012, et à la Direction de l'AIPRP d'ici le 24 août.

Plan d'action de la gestion 1.3.1 : La DGSMPS travaillera en collaboration avec la Direction générale de la surveillance (DGS) et la DGSIT afin de procéder à un examen de la sécurité à l'égard du type de renseignements classifiés qui sont traités électroniquement au sein de la DACT, en vue d'identifier les processus pertinents en matière de classification, de création, d'entreposage et de transmission des renseignements

Cette mesure sera mise en œuvre au plus tard le 31 octobre 2012.

Plan d'action de la gestion 1.3.2 : La DGSMPS travaillera en collaboration avec la DGS et la DGSIT, au besoin, pour concevoir et mettre en place des solutions pertinentes fondées sur les risques, sur la base des résultats de l'examen de la sécurité. Les procédures internes de la DACT qui seront élaborées à l'issue de la mesure indiquée en 1.1 seront également mises à jour, au besoin, afin de refléter les résultats de l'examen de la sécurité.

Cette mesure sera mise en œuvre au plus tard le 30 décembre 2012.

Recommandation 2 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait vérifier la disponibilité des systèmes de TI classifiés de la DGSMPS afin de s'assurer qu'ils répondent aux besoins opérationnels.

Plan d'action de la gestion 2.1 : La DGSMPS passera en revue les exigences opérationnelles liées à ses systèmes classifiés de TI et en fera part à la DGSIT, au besoin, afin d'assurer le respect de ses besoins opérationnels.

Cette mesure a été réalisée pour la DACT en février 2012 et sera mise en œuvre par la Direction de l'AIPRP au plus tard le 27 avril 2012.

Recommandation 3 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait établir des mesures pour veiller à ce que seules les personnes ayant une autorisation de sécurité appropriée et ayant besoin d'un accès afin d'accomplir leurs tâches, aient accès aux systèmes de TI classifiés de la DGSMPS.

> **Plan d'action de la gestion 3.1 :** La DACT et la Direction de l'AIPRP passeront en revue, sur une base trimestrielle, la liste des utilisateurs actifs (rapport de système) tirée de leurs systèmes classifiés de TI afin d'en valider l'autorisation. Ces directions devront par le fait même demander à la DGSIT de valider la liste et les autorisations des employés de la DGSIT qui ont accès à leurs systèmes.
>
> Cette mesure sera mise en œuvre sur une base trimestrielle à compter du 30 avril 2012.

Recommandation 4 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce que les supports électroniques de la DGSMPS, y compris sans s'y limiter, les disques durs d'ordinateur, les clés USB et les disquettes pouvant contenir des renseignements classifiés, soient marqués comme il se doit.

> **Plan d'action de la gestion 4.1 :** La DGSMPS élaborera des procédures afin de veiller à ce que tous les supports électroniques, l'équipement et les appareils pouvant contenir des renseignements classifiés soient identifiés comme il se doit. Ces procédures contiendront également des dispositions portant sur le marquage adéquat des supports électroniques, de l'équipement et des appareils qui sont hors site et dont la DGSMPS assure le contrôle.
>
> Cette mesure sera mise en œuvre à la DPSAC au plus tard le 31 mai 2012, à la Direction de l'AIPRP d'ici le 29 juin 2012 et à la DACT d'ici le 30 septembre 2012.

Recommandation 5 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce qu'une procédure complète et détaillée s'adressant aux personnes devant procéder à l'élimination du matériel pouvant contenir des renseignements classifiés soit élaborée et diffusée.

> **Plan d'action de la gestion 5.1 :** La DGSMPS travaillera en collaboration avec la DGSIT et la DGS, au besoin, afin de passer en revue les lignes directrices en vigueur à l'échelle du Ministère sur l'élimination du matériel électronique et de

les modifier, au besoin, de façon à aider les propriétaires ou les organismes gardiens à éliminer le matériel classifié à TPSGC.

Cette mesure sera mise en œuvre au plus tard le 28 septembre 2012.

Plan d'action de la gestion 5.2 : La DGSMPS diffusera les procédures à l'échelle de TPSGC au moyen de communiqués.

Cette mesure sera mise en œuvre au plus tard le 31 octobre 2012.

Recommandation 6 : La sous-ministre adjointe, Direction générale de la surveillance, en collaboration avec le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait procéder à une analyse afin de déterminer si les observations et les recommandations de la vérification contenues dans le présent rapport s'appliquent à d'autres unités opérationnelles de TPSGC et, le cas échéant, fournir une orientation fonctionnelle afin de combler les lacunes décelées.

Plan d'action de la gestion 6.1 : Les ministères sont chargés de choisir, de mettre en œuvre et de maintenir des mesures durables de contrôle de la sécurité afin d'atteindre les objectifs établis à ce chapitre. Les contrôles de sécurité peuvent être relatifs à la gestion, de nature administrative, opérationnelle, technique ou procédurale. Les contrôles obligatoires et recommandés sont précisés dans les normes et lignes directrices qui appuient la Politique sur la sécurité du gouvernement. Les ministères peuvent prendre d'autres mesures de contrôle de sécurité et se fixer des objectifs additionnels en se fondant sur les résultats des évaluations des risques. La Directive sur la gestion de la sécurité ministérielle du Conseil du Trésor définit les mesures de contrôle de sécurité qui devraient être comprises dans un programme de sécurité ministérielle efficace.

Examen du Programme de sécurité du Ministère

Le Programme de sécurité du Ministère doit faire l'objet d'un examen exhaustif au moyen des objectifs en matière de contrôle de sécurité établis dans la Directive sur la gestion de la sécurité ministérielle, notamment :

- assurance de l'information;
- enquêtes de sécurité;
- sécurité matérielle;
- sécurité des TI et systèmes de TI;
- sécurité des marchés;
- partage de renseignements et de biens avec d'autres administrations publiques et organisations;
- obtention de services de sécurité auprès d'autres organisations;
- sensibilisation aux questions de sécurité;
- formation sur la sécurité;

- gestion des incidents de sécurité;
- protection des employés contre la violence en milieu de travail,
- inspections de sécurité;
- enquêtes administratives liées aux incidents de sécurité;
- sécurité dans les situations d'urgence et de menace accrue;
- planification des urgences et de la continuité des activités.

L'examen de la sécurité visera les directions générales du Ministère, ainsi que les organismes de service spéciaux et les régions.

Évaluation des menaces et des risques pour l'architecture des activités de programme et profil des risques liés à la sécurité

Une évaluation des menaces et des risques pour l'architecture des activités de programme du Ministère sera réalisée, puisqu'il existe des risques qui pourraient avoir des répercussions sur la capacité de ce dernier d'offrir ses services et d'exécuter ses programmes. L'évaluation fournira une analyse descendante des risques à la sécurité inhérents aux activités de programme du Ministère menées par les directions générales, les organismes de service spéciaux et les régions.

L'examen des programmes et l'évaluation des menaces et des risques seront réalisés conjointement, puisque ces activités sont interreliées.

INTRODUCTION

1. L'information ou renseignements de nature délicate est l'information qui doit être protégée, car sa divulgation, son altération, sa perte ou sa destruction pourrait porter préjudice à des biens ou des personnes. Il existe deux types d'information de nature délicate au gouvernement du Canada : les renseignements protégés et les renseignements classifiés. Les renseignements protégés sont les renseignements n'étant pas d''intérêt national. Les renseignements protégés peuvent être des renseignements personnels, comme des examens annuels de rendement du personnel ou des données bancaires sur les dépôts de la paie. Les catégories de protection sont les suivantes : Protégé A, Protégé B et Protégé C. Les renseignements classifiés correspondent à l'information de nature délicate dont la divulgation non autorisée risquerait vraisemblablement de porter préjudice à l'intérêt national, c'est-à-dire à la sécurité et à la stabilité sociale, politique et économique du Canada. Par exemple, les mémoires au Cabinet sont considérés comme des documents classifiés. Les catégories de classification sont, par ordre croissant de sensibilité : Confidentiel, Secret et Très secret. Le traitement des renseignements électroniques classifiés comprend entre autres la création, l'entreposage, la transmission et la destruction des renseignements classifiés.

2. Les renseignements confidentiels du Cabinet sont des sources importantes de renseignements classifiés au sein de TPSGC. Il est important de protéger la confidentialité de ces documents pour garantir le fonctionnement adéquat du processus décisionnel du Cabinet. Cela permet aux ministres d'échanger leurs vues et leurs opinions sur des questions de politique afin de parvenir à un consensus. Les renseignements confidentiels du Cabinet comprennent les versions provisoires et finales des documents du Cabinet et du Conseil du Trésor, les mémoires au Cabinet, les présentations au Conseil du Trésor ainsi que les documents d'information, les exposés ou les notes de service qui ont trait à des documents du Cabinet ou du Conseil du Trésor. Tous les documents du Cabinet sont classifiés. Les présentations au Conseil du Trésor sont des documents classifiés ou protégés, selon la sensibilité de leur contenu.

3. Diverses directions générales de TPSGC dirigent, créent ou examinent les mémoires au Cabinet et les présentations au Conseil du Trésor. La Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC) et la Direction des affaires relatives au Conseil du Trésor (DACT), qui font partie de la Direction générale des services ministériels et des politiques stratégiques (DGSMPS), fournissent aux agents de TPSGC un centre d'expertise pour les aider à créer les documents du Cabinet et les présentations au Conseil du Trésor qui ont trait aux initiatives de TPSGC. De plus, avant chaque réunion du Cabinet, la DPSAC informe le ministre de TPSGC de tous les points pertinents qui doivent être abordés.

4. La Direction de l'accès a l'information et de la protection des renseignements personnels (AIPRP) de la DGSMPS administre la *Loi sur l'accès à l'information* et la *Loi sur la protection des renseignements personnels* au nom du Ministère. Elle traite

ainsi des renseignements classifiés comme les documents du Cabinet et du Conseil du Trésor ainsi que les éléments d'information connexes.

5. Le Bureau du Conseil privé, le Secrétariat du Conseil du Trésor du Canada, les organismes responsables de la sécurité, comme la Gendarmerie royale du Canada, et TPSGC ont créé une série d'instruments de politique qui contiennent les exigences à respecter pour protéger les renseignements classifiés traités par voie électronique au sein de TPSGC. Les principaux instruments de politique qui portent sur le traitement électronique des renseignements classifiés incluent :

   - la *Politique sur la sécurité des documents confidentiels du Cabinet* de 2007 publiée par le Bureau du Conseil privé, qui décrit les mesures de sécurité à respecter pour éviter que le contenu des documents confidentiels du Cabinet ne soit divulgué à des personnes non autorisées;

   - la *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)* de 2004, publiée par le Secrétariat du Conseil du Trésor du Canada, qui définit les exigences de sécurité de base que les ministères fédéraux doivent respecter pour protéger les renseignements et les biens liés à la technologie de l'information dont ils sont responsables;

   - la *Politique ministérielle (PM) 055 – Programme de sécurité de la technologie de l'information de 2003,* qui décrit le Programme de sécurité de la technologie de l'information (TI), définit les rôles connexes et établit les mesures de protection nécessaires pour assurer la confidentialité, l'intégrité et la disponibilité des renseignements ainsi que des systèmes et des services connexes. En juillet 2010, cette politique a été remplacée par la *Politique ministérielle (PM) 104 - Politique sur la sécurité des technologies de l'information*. Puisque la portée de la vérification chevauchait cette date, les deux politiques ministérielles ont été prises en compte au cours de la vérification.

6. Le Programme de sécurité du Ministère vise à assurer la coordination des fonctions liées à la sécurité et à mettre en œuvre les exigences de sécurité au sein de TPSGC. Il est appuyé par le Programme de la sécurité ministérielle et le Programme de sécurité des technologies de l'information (TI) du Ministère. Le Programme de la sécurité ministérielle établit la politique et le cadre ministériels de la sécurité matérielle et de la protection des biens importants, y compris les renseignements personnels et l'information de nature délicate. Le Programme de sécurité de la TI du Ministère veille à la sécurité des renseignements électroniques des biens de TI et des services connexes du Ministère.

7. Jusqu'au 15 novembre 2011, la sous-ministre adjointe de la Direction générale des services ministériels et des politiques stratégiques était chargée d'administrer le Programme de sécurité du Ministère. Cette responsabilité est maintenant assumée par la sous-ministre adjointe de la Direction générale de la surveillance, qui est également chargée de diriger le Programme de la sécurité ministérielle. La sous-ministre

adjointe de la Direction générale des services ministériels et des politiques stratégiques est responsable d'élaborer un cadre de gestion des biens de TI et de gérer l'élimination des biens de TI conformément à ce cadre.

8. La Direction générale des services d'infotechnologie a la responsabilité générale du Programme de sécurité des technologies de l'information (TI) du Ministère. Le Dirigeant principal de l'information, Direction générale des services d'infotechnologie, est chargé d'administrer ce programme. Il doit entre autres élaborer et tenir à jour des cadres de sécurité de l'infrastructure et des applications de TI, élaborer et publier des directives, des procédures et des normes de sécurité relatives à l'infrastructure, aux application et aux opérations de TI. Il doit aussi mesurer l'efficacité du programme de protection et de certification de l'infrastructure et des applications de TI et en informer les responsables de la certification ainsi que sensibiliser les utilisateurs à la sécurité des TI en ce qui concerne les applications, les opérations et l'infrastructure, et leur donner une formation connexe. Le coordonnateur de la sécurité des TI de la Direction générale des services d'infotechnologie est chargé d'établir et de gérer le Programme de sécurité de la TI du Ministère. Il doit entre autres concevoir, mettre en œuvre et promouvoir un programme de sensibilisation à la sécurité des TI, et travailler en étroite collaboration avec les gestionnaires de programmes et de services pour veiller à satisfaire les besoins en matière de sécurité des TI. Il doit également fournir des conseils sur les mesures de protection et les informer du risque résiduel d'un programme ou d'un service.

9. Les responsables de direction générale sont en charge du financement et de l'appliquation, au sein de leur organisation, des programmes et des mesures de sécurité qui ont été approuvés par TPSGC. Bien que les gestionnaires de la prestation de programmes et services puissent déléguer la responsabilité de la sécurité des TI à des experts techniques, ils sont tout de même tenus de rendre compte au sous-ministre et sont responsables d'assurer la sécurité des programmes et des services qui relèvent de leur autorité.

10. En plus d'être responsable du Programme de sécurité des technologies de l'information du Ministère, la Direction générale des services d'infotechnologie fournit un soutien en matière de technologie de l'information à de nombreux systèmes de TI de TPSGC, y compris ceux qu'utilisent les entités vérifiées pour traiter des renseignements électroniques classifiés.

OBJECTIF DE LA VÉRIFICATION

11. Cette vérification interne visait à déterminer si certaines directions de la Direction générale des services ministériels et des politiques stratégiques traitaient les renseignements classifiés électroniques conformément à certaines exigences figurant dans les instruments de politique.

12. Trois directions de la Direction générale des services ministériels et des politiques stratégiques ont été sélectionnées pour cette vérification, en raison du risque qu'elles représentent : la Direction des affaires relatives au Conseil du Trésor (DACT), la Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC) et la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP). Ces directions traitent des renseignements classifiés dans le cadre de la prestation de services au Ministère.

13. La vérification a permis de déterminer le degré de conformité dans six principaux secteurs d'exigences liés à la création, à l'entreposage, à la transmission et à la destruction des renseignements électroniques classifiés. Elle portait en particulier sur les secteurs suivants :
    - le matériel de TI utilisé pour créer et entreposer des renseignements électroniques classifiés;
    - la transmission des renseignements électroniques classifiés;
    - les autorisations de sécurité des personnes qui traitent les renseignements électroniques classifiés;
    - le marquage de sécurité des renseignements électroniques classifiés et des supports de TI;
    - la zone de sécurité matérielle dans laquelle les renseignements électroniques classifiés sont traités;
    - la destruction ou l'élimination du matériel électronique utilisé pour traiter des renseignements électroniques classifiés.

14. Pour obtenir plus de renseignements sur l'objectif, l'étendu, la méthode et les critères, voir la section « À propos de la vérification », à la fin du présent rapport.

ÉNONCÉ D'ASSURANCE

15. La présente vérification a été réalisée conformément aux *Normes internationales pour la pratique professionnelle de la vérification interne* de l'Institut des vérificateurs internes. Des procédures de vérification suffisantes et appropriées ont été suivies et des éléments probants ont été recueillis pour appuyer l'exactitude des constatations et des conclusions énoncées dans le présent rapport et fournir une assurance de niveau de vérification. Les constatations et les conclusions sont axées sur une comparaison des conditions telles qu'elles existaient alors, aux critères de vérification préétablis qui ont été acceptés par la gestion. Les constatations et les conclusions s'appliquent seulement aux entités vérifiées ainsi qu'à l'étendue et la période visées par la vérification.

OBSERVATIONS

SYSTÈMES DE TI CLASSIFIÉS

Les renseignements électroniques classifiés n'étaient pas toujours créés, entreposés et transmis dans un système de TI adéquat

16. La *Politique ministérielle (PM) 104 – Politique sur la sécurité des technologies de l'information*, établit qu'il est interdit de transmettre des renseignements classifiés sur le réseau principal de TPSGC. La *Politique sur la sécurité des documents confidentiels du Cabinet* stipule que les renseignements secrets ou confidentiels du Cabinet doivent être traités uniquement par l'entremise d'un réseau Secret, d'un système autonome ou d'un lecteur ministériel dédié uniquement aux personnes qui travaillent sur les documents confidentiels du Cabinet. Elle stipule également que ces systèmes doivent être dotés de dispositifs de sécurité efficaces contre l'accès de personnes non autorisées, et que les documents confidentiels du Cabinet ne doivent pas être transmis par courriel à moins qu'ils ne soient destinés à d'autres utilisateurs du même réseau classifié. Conformément à ces exigences, les renseignements secrets ou confidentiels, y compris les documents confidentiels du Cabinet, peuvent être traités sur des ordinateurs autonomes dotés de mesures de contrôle approuvées ou sur des réseaux locaux spéciaux distincts.

17. Un réseau local est un réseau qui s'étend sur une zone relativement restreinte, comme un édifice ou un groupe d'édifices. Un ordinateur autonome est un ordinateur qui n'est pas relié à d'autres ordinateurs ou réseaux. De même, un réseau local distinct est un réseau local qui n'est pas relié à d'autres réseaux. Un ordinateur autonome doté des mesures de contrôle approuvées, ou un réseau local spécial distinct conçu pour le traitement des renseignements classifiés peut être appelé « système de TI classifié ».

18. En traitant des renseignements classifiés sur un ordinateur qui n'est pas relié à d'autres ordinateurs ou à d'autres réseaux ou sur un réseau local qui n'est pas relié à d'autres réseaux, on limite les moyens d'accéder au système, ce qui facilite l'élimination des accès non autorisés. Il est aussi important que l'ordinateur ou le réseau local qui sert à traiter les renseignements classifiés soit prévu pour cet usage. Ces ordinateurs et réseaux sont dotés de mesures de contrôle et de protection qui permettent de protéger les renseignements classifiés des accès non autorisés. Il se peut que les ordinateurs et les réseaux qui ne sont pas destinés au traitement des renseignements classifiés ne soient pas dotés de mesures de contrôle et de protection suffisantes pour protéger l'information comme il se doit. Par conséquent, pour réduire le risque d'accès non autorisé aux renseignements électroniques classifiés, il est important que les renseignements classifiés soient traités sur un système de TI approprié, soit un ordinateur autonome ou un réseau local spécial distinct qui est prévu pour le traitement de ces renseignements. Il est aussi important que les courriels qui contiennent des renseignements classifiés soient uniquement transmis aux utilisateurs d'un même réseau classifié.

19. Nous nous attendions à ce que les renseignements électroniques classifiés soient uniquement traités sur des systèmes de TI appropriés, comme des ordinateurs autonomes dotés de mesures de contrôle approuvées ou sur des réseaux locaux

spéciaux distincts. Nous nous attendions aussi à ce que le système de TI utilisé pour traiter les renseignements électroniques classifiés soit destiné à cette fin.

20. Nous avons constaté que la DPSAC et la Direction de l'AIPRP traitaient des renseignements électroniques classifiés sur des réseaux locaux spéciaux distincts qui sont destinés aux renseignements classifiés. Le réseau local utilisé par la DPSAC était disponible du lundi au vendredi, de 6 h à 18 h 30. Ce système était inaccessible en dehors de ces heures, sauf si les usagers demandaient d'avance une prolongation des heures. Or, des prolongations n'étaient pas toujours demandées, et nous avons constaté que lorsque des personnes de la DPSAC faisaient des heures supplémentaires pour respecter les échéances liées aux documents du Cabinet, elles transféraient des renseignements classifiés de leur système de TI classifié vers leur ordinateur de bureau ordinaire relié au réseau de TPSGC. Ce réseau n'est pas destiné aux renseignements classifiés mais aux renseignements « Protégé B » encodés et aux renseignements jusqu'au niveau de sécurité « Protégé A ».

21. Nous avons aussi constaté que des personnes qui travaillaient pour la DACT n'avaient pas accès à un système de TI classifié et qu'elles traitaient des renseignements classifiés sur des ordinateurs reliés au réseau de TPSGC.

22. Enfin, nous avons remarqué que le réseau de TPSGC était parfois utilisé par des membres de la DACT ou de la DPSAC pour communiquer des renseignements classifiés allant jusqu'au niveau « Secret ». Certaines personnes ont affirmé qu'elles utilisaient le réseau de TPSGC pour envoyer des renseignements classifiés lorsqu'elles ne partageaient pas un réseau classifié avec leurs destinataires et le temps ne permettait pas d'utiliser un messager autorisé pour envoyer l'information.

23. L'information créée, entreposée ou transmise sur le réseau de TPSGC peut devenir accessible aux personnes qui ont accès au réseau. Le fait d'utiliser un système de TI classifié pour traiter des renseignements électroniques classifiés aide à éliminer l'accès non autorisé aux renseignements électroniques classifiés.

GESTION DES SYSTÈMES DE TI CLASSIFIÉS ET DES RENSEIGNEMENTS CLASSIFIÉS

Les systèmes de TI classifiés utilisés par DPSAC et la Direction de l'AIPRP ne détenaient pas de certification ou d'accréditation à jour

24. Selon la norme de *Gestion de la sécurité des technologies de l'information* (GSTI), publiée en 2004, les ministères sont tenus d'obtenir la certification et l'accréditation pour leurs systèmes de TI. La certification sert à s'assurer que les exigences de sécurité établies pour un système particulier sont respectées et que les contrôles et mesures de protection fonctionnent comme prévu. Le terme « accréditation » signifie que la gestion a autorisé l'exploitation du système ou du service et qu'elle a accepté

le risque résiduel qui en découle, en se fondant sur les éléments probants de la certification.

25. Il convient de revoir périodiquement les certifications et les accréditations des systèmes de TI pour veiller à ce qu'elles tiennent compte des changements liés aux risques et aux systèmes. Les certifications et les accréditations sont en vigueur pendant la période précisée dans la lettre de certification ou d'accréditation. Une certification et une accréditation valides contribuent à s'assurer qu'un système dispose de mesures de contrôle et de protection suffisantes pour protéger l'information de façon adéquate, et qu'il respecte les normes du gouvernement du Canada. Autrement, il y aurait risque que le système de TI ne soit pas doté des mesures suffisantes pour protéger l'information de façon adéquate, ce qui comporterait un risque pour la confidentialité, l'intégrité et la disponibilité de l'information.

26. Nous nous attendions à ce que les réseaux locaux distincts ou les systèmes de TI classifiés, destinés au traitement des renseignements électronique classifiés de la DPSAC et de la Direction de l'AIPRP, aient été certifiés et accrédités selon le niveau de sécurité approprié. Nous nous attendions également à ce que la certification et l'accréditation soient valides au moment de la vérification.

27. Nous avons constaté que le système de TI classifié utilisé par la DPSAC pour traiter des renseignements classifiés avait été certifié; toutefois, cette certification avait pris fin en 2004. Nous n'avons trouvé aucun élément probant nous permettant de conclure que le système de TI classifié de la DPSAC était accrédité. Nous avons également constaté que le système de TI classifié utilisé par la Direction de l'AIPRP avait été certifié et accrédité pour traiter de l'information au niveau de sécurité approprié; cependant, l'accréditation avait expiré en 2006 et la certification avait expiré en 2007. Comme les membres de la DACT n'avaient pas accès à un système de TI classifié, nous n'avons pas examiné la certification et l'accréditation du système utilisé par la DACT.

28. Les systèmes de TI peuvent changer avec le temps, en raison de la maintenance et de l'évolution. Une certification et une accréditation à jour aident à s'assurer que les systèmes de TI ont des mécanismes de contrôle et de protection suffisants pour gérer les risques actuels liés à l'accès non autorisé.

La mise à jour administrative des comptes d'utilisateurs était inadéquate

29. La *Politique ministérielle (PM) 104 - Politique sur la sécurité des technologies de l'information* exige qu'un identificateur d'utilisateur unique soit attribué à chaque utilisateur, et que cet identificateur ne soit valide que durant l'emploi de la personne ou le temps qu'elle en a besoin pour effectuer une tâche donnée.

30. Les utilisateurs ont accès aux systèmes informatiques par l'entremise de comptes d'utilisateur et établissent leur identité au moyen d'un identificateur. Les

identificateurs peuvent être soit génériques, soit uniques. Un identificateur unique est attribué à un seul utilisateur. Un identificateur générique peut être utilisé par deux utilisateurs ou plus ou attribué à un seul puis, lorsque celui-ci n'a plus besoin de son compte d'utilisateur, être réattribué à un nouvel utilisateur.

31. Les identificateurs génériques compliquent le contrôle d'accès au système. Leur utilisation fait également en sorte qu'il est plus difficile de retracer les activités et d'établir le lien entre elles et les personnes. Afin de réduire le risque d'accès non autorisé aux systèmes de TI classifiés, il est important d'éviter de recourir aux identificateurs génériques. En outre, lorsque les personnes n'ont plus besoin d'accéder aux systèmes de TI classifiés dans l'exercice de leurs fonctions, il est important de leur en retirer l'accès, en désactivant leurs identificateurs d'utilisateur. Cela réduit davantage le risque d'accès non autorisé.

32. Nous nous attendions à ce qu'un identificateur unique ait été attribué à chaque utilisateur, et que les identificateurs génériques n'aient pas été utilisés avec les systèmes de TI classifiés. Nous nous attendions également à ce que chaque identificateur n'ait été valide que durant l'emploi de la personne ou le temps qu'elle en ait eu besoin pour effectuer une tâche donnée.

33. Nous avons constaté que le nombre d'identificateurs d'utilisateur actifs destinés au personnel de la DPSAC ayant accès au système de TI classifié était supérieur au nombre d'employés actuels qui utilisent le système. Ces identificateurs supplémentaires étaient attribués à des personnes qui avaient quitté l'organisation. En outre, le système de TI classifié de la DPSAC ainsi que celui de la Direction de l'AIPRP comptaient un certain nombre d'identificateurs génériques. Nous n'avons pas été en mesure de déterminer qui avait accès à certains identificateurs génériques destinés aux administrateurs de système.

34. Le fait de limiter l'utilisation d'identificateurs génériques et de s'assurer que les identificateurs ne sont valides que durant l'emploi des personnes ou le temps qu'elles en ont besoin pour effectuer une tâche donnée aide à restreindre l'accès non autorisé aux renseignements électroniques classifiés.

Les personnes identifiées comme ayant accès aux systèmes de TI classifiés avaient une autorisation de sécurité adéquate

35. Une autorisation de sécurité indique que l'évaluation de la sécurité a été achevée avec succès. Cette autorisation permet à son détenteur d'accéder aux renseignements classifiés selon le besoin de connaître. Le Canada a trois niveaux d'autorisation de sécurité : Confidentiel, Secret et Très secret. La *Politique sur la sécurité du gouvernement* exige que toutes les personnes qui auront accès à des renseignements classifiés obtiennent une autorisation de sécurité appropriée avant le début de l'exercice de leurs fonctions.

36. Il est important que les personnes qui ont accès à des renseignements classifiés aient une autorisation de sécurité appropriée, laquelle indique qu'elles ont fait l'objet d'un contrôle de sécurité au niveau approprié et qu'elles rencontrent les exigences qui y sont associées. Cela contribue à s'assurer que seules les personnes dont la loyauté et la fiabilité ont été déterminées sont autorisées à accéder à des renseignements classifiés.

37. Nous nous attendions à ce que les personnes qui avaient accès à des renseignements électroniques classifiés aient une autorisation de sécurité appropriée.

38. Nous avons constaté que toutes les personnes qui travaillaient au sein de la DACT, la DPSAC et la Direction de l'AIPRP avaient une autorisation de sécurité appropriée. Les personnes qui, selon nos observations, avaient accès aux systèmes de TI classifiés à des fins administratives avaient également une autorisation de sécurité appropriée.

39. Cependant, nous n'avons pas été en mesure de déterminer qui avait accès à certains des identificateurs d'utilisateur génériques destinés aux administrateurs du système. Par conséquent, nous ne savons pas si les personnes qui avaient accès à ces identificateurs d'utilisateur génériques avaient toutes une autorisation de sécurité appropriée.

40. Pour contribuer à atténuer les risques d'accès non autorisé à des renseignements électroniques classifiés, il est important de s'assurer que les personnes qui ont accès aux systèmes de TI classifiés ont une autorisation de sécurité appropriée.

Le marquage des documents était adéquat, mais celui des supports de TI n'était pas fait de façon systématique.

41. Le marquage de sécurité désigne l'étiquetage des dossiers classifiés et protégés (documents papier et électronique) et des supports de TI, à savoir le matériel électronique utilisé pour entreposer l'information. La *Politique sur la sécurité des documents confidentiels du Cabinet* établit les exigences relatives au marquage des documents du Conseil du Trésor et des renseignements confidentiels du Cabinet. En outre, la norme de la *Gestion de la sécurité des technologies de l'information (GSTI)* exige que les supports de TI contenant des renseignements classifiés soient également marqués.

42. Il est important de bien étiqueter les renseignements classifiés et les supports de TI utilisés pour entreposer ces renseignements; cela permet aux personnes de connaître le niveau de sécurité des biens et de les protéger adéquatement. L'auteur de l'information de nature délicate est normalement responsable du marquage du document et des autres supports. Nous nous attendions à ce que les directions aient marqué de façon appropriée les renseignements électroniques classifiés qu'elles avaient créés de même que les supports de TI utilisés pour entreposer ces renseignements.

43. Nous avons examiné un échantillon de renseignements électroniques classifiés créés par la DPSAC et la Direction de l'AIPRP. Nous avons également examiné un échantillon de supports de TI utilisés par les directions pour traiter et entreposer les renseignements électroniques classifiés. Bien que la DACT traite des renseignements électroniques classifiés, elle a indiqué qu'elle ne les créait pas. De plus, la direction ne possédait aucun support électronique classifié, étant donné qu'elle ne disposait pas d'un système de TI classifié.

44. Nous avons constaté que :
    - La DPSAC et la Direction de l'AIPRP marquaient de manière appropriée les renseignements électroniques classifiés qu'elles créaient;
    - Dans l'ensemble, les supports électroniques de la DPSAC et de la Direction de l'AIPRP n'étaient pas marqués de façon systématique.

45. Le marquage des renseignements électroniques classifiés permet aux personnes de connaître le niveau de sensibilité de l'information. Le marquage des supports de TI permet également aux personnes de connaître le niveau de sensibilité des supports et de l'information qu'ils contiennent.

Les zones de sécurité matérielle étaient appropriées

46. Les zones sont des espaces clairement reconnaissables utilisés pour en contrôler l'accès. La *Norme opérationnelle sur la sécurité matérielle,* publiée par le Secrétariat du Conseil du Trésor du Canada, définit une hiérarchie des zones. Ces zones permettent aux ministères de protéger l'information et les biens de divers niveaux de sensibilité, en fonction des différents niveaux de menace dans une même installation. À cette norme s'ajoute le *Guide pour l'établissement des zones de sécurité matérielle* publié par la Gendarmerie royale du Canada (GRC). Ce guide décrit les pratiques exemplaires qui visent à réduire le risque d'événements indésirables. Il recommande qu'au minimum, les renseignements secrets soient traités, entreposés ou détruits dans une zone de sécurité matérielle.

47. Pour veiller à ce que les mesures de protection matérielle minimales exigées pour protéger les informations classifiées soient en place et pour réduire le risque d'accès non autorisé, les renseignements classifiés doivent être traités et entreposés dans une zone de sécurité matérielle appropriée.

48. Nous nous attendions à ce que les directions traitent et entreposent les renseignements électroniques classifiés dans une zone de sécurité matérielle appropriée, c'est-à-dire, une zone qui répond aux exigences minimales décrites dans le *Guide pour l'établissement des zones de sécurité matérielle.*

49. Nous avons constaté que la DACT, la DPSAC et la Direction de l'AIPRP, ainsi que les systèmes de TI classifiés utilisés par la DPSAC et la Direction de l'AIPRP pour traiter des renseignements classifiés, étaient situés dans des zones de sécurité matérielle appropriée.

50. Traiter les renseignements électroniques classifiés dans une zone de sécurité matérielle appropriée aide à atténuer les risques d'accès non autorisé aux renseignements électroniques classifiés en veillant à ce que des mécanismes de contrôle matériel appropriés soient en place.

Le matériel électronique classifié n'avait pas été éliminé

51. Plusieurs méthodes de sécurité sont utilisées pour protéger les renseignements de nature délicate lorsqu'ils sont traités et entreposés dans les systèmes de TI; cependant, il est possible de récupérer de l'information de nature délicate dans le matériel mis au rebut.

52. Nous nous attendions à ce que le matériel contenant des renseignements électroniques classifiés ait été éliminé selon des méthodes et des procédures appropriées.

53. Nous avons constaté que, durant la période couverte par la vérification, la DACT, la DPSAC et la Direction de l'AIPRP n'avaient pas éliminé le matériel électronique classifié, c'est-à-dire le matériel électronique contenant des renseignements classifiés. Alors que la DACT n'avait pas d'équipement classifié à éliminer, la DPSAC et la Direction de l'AIPRP avaient entreposé du matériel électronique classifié qui n'était plus utilisé. Même si un processus d'élimination de matériel électronique était documenté, l'information fournie dans ce document n'était pas suffisamment détaillée pour appuyer les propriétaires ou les organismes gardiens concernant l'élimination du matériel classifié à TPSGC. Par conséquent, le matériel électronique classifié n'avait pas été éliminé.

54. Une procédure complète et détaillée à l'intention des propriétaires et des organismes gardiens de matériel électronique classifié contribuerait à faire en sorte que le matériel ne soit pas entreposé pour de longues périodes. En outre, elle contribuerait à assurer la protection des données que contient ce matériel.

CONCLUSION

55. Les directions sélectionnées au sein de la Direction générale des services ministériels et des politiques stratégiques ne traitaient pas toujours les renseignements électroniques classifiés de manière conforme aux exigences des instruments de politique. Le fait de traiter les renseignements électroniques classifiés conformément aux instruments de politique contribue à protéger l'information contre l'accès non autorisé et à assurer la confidentialité, l'intégrité et la disponibilité des renseignements.

56. Nous avons constaté que deux des trois directions ayant fait l'objet de la vérification traitaient des renseignements électroniques classifiés à l'aide de systèmes de TI classifiés, alors que la troisième n'avait pas accès à un système de TI classifié pour protéger ses renseignements. Par conséquent, les renseignements électroniques

classifiés étaient traités au moyen d'ordinateurs de bureau ordinaires reliés au réseau de TPSGC, lequel n'a pas été conçu à cette fin. Nous avons également constaté que le réseau de TPSGC était parfois utilisé par des membres de la DACT et de la DPSAC pour partager des renseignements classifiés allant jusqu'au niveau « Secret ».

57. Nous avons constaté que la DPSAC et la Direction de l'AIPRP n'avaient pas de certification et d'attestation pour leurs systèmes de TI classifiés au moment de la vérification. Nous avons aussi constaté qu'il y avait, pour un des systèmes de TI classifiés, des identificateurs d'utilisateur actifs attribués à des personnes qui ne travaillaient plus pour l'organisation, et que les deux systèmes de TI utilisaient des identificateurs d'utilisateur génériques.

58. Nous avons constaté que les personnes identifiées comme ayant accès aux systèmes de TI classifiés avaient une autorisation de sécurité adéquate. Cependant, nous n'avons pas été en mesure de déterminer qui avait accès à certains des identificateurs d'utilisateur génériques. Par conséquent, nous ne savons pas si les personnes qui avaient accès à ces identificateurs d'utilisateur génériques avaient toutes une autorisation de sécurité appropriée. Nous avons noté que les renseignements électroniques classifiés créés par les directions étaient marqués de façon appropriée. Toutefois, le matériel de TI utilisé pour traiter ces renseignements n'était pas marqué de façon systématique. Nous avons également noté que les trois directions sélectionnées pour la vérification traitaient des renseignements électroniques classifiés dans des zones de sécurité matérielle appropriées. Enfin, nous avons constaté qu'aucun processus officiel n'était en place pour l'élimination du matériel électronique classifié qui n'était plus utilisé.

RÉPONSE DE LA GESTION

La direction reconnaît que les constatations du rapport sont justes et exactes en ce qui concerne la façon dont les renseignements électroniques classifiés ont été traités par les trois directions visées par la vérification.

La direction donnera suite aux recommandations contenues dans le rapport de vérification en mettant en place le Plan d'action de la gestion suivant.

RECOMMANDATIONS ET PLAN D'ACTION DE LA GESTION

Recommandation 1 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce que les renseignements électroniques classifiés de la DGSMPS soient créés, entreposés et transmis uniquement dans des systèmes de TI adéquats, et que ces systèmes restent certifiés et accrédités au niveau approprié.

Plan d'action de la gestion 1.1 : La Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC), la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP) et la Direction des affaires relatives au Conseil du Trésor (DACT) élaboreront et mettront en place des procédures internes liées à la création, à l'entreposage et à la transmission des renseignements électroniques classifiés, y compris des procédures de traitement des renseignements classifiés, si les systèmes classifiés de TI ne sont pas disponibles.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 31 mai 2012, à la Direction de l'AIPRP au plus tard le 31 juillet 2012, et à la DACT au plus tard le 31 décembre 2012.

Plan d'action de la gestion 1.2.1 : En tant que propriétaire de système d'affaires, la DGSMPS, en collaboration avec le coordonnateur de la sécurité de la TI, élaborera un plan de certification afin de faire accréditer les systèmes désignés ainsi que l'infrastructure connexe.

Plan d'action de la gestion 1.2.2 : Fournir au coordonnateur de la sécurité de la TI les éléments de preuve requis, tel que décrit dans le plan de certification, afin d'appuyer la réalisation du processus de certification et d'accréditation.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 28 septembre 2012, et à la Direction de l'AIPRP d'ici le 29 juin 2012.

Plan d'action de la gestion 1.2.3 : La DGSMPS signera la lettre d'accréditation soumise par le coordonnateur de la sécurité de la TI afin d'accepter les recommandations relatives au traitement des risques résiduels.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 30 novembre 2012, et à la Direction de l'AIPRP d'ici le 24 août.

Plan d'action de la gestion 1.3.1 : La DGSMPS travaillera en collaboration avec la Direction générale de la surveillance (DGS) et la DGSIT afin de procéder à un examen de la sécurité à l'égard du type de renseignements classifiés qui sont traités électroniquement au sein de la DACT, en vue d'identifier les processus pertinents en matière de classification, de création, d'entreposage et de transmission des renseignements

Cette mesure sera mise en œuvre au plus tard le 31 octobre 2012.

Plan d'action de la gestion 1.3.2 : La DGSMPS travaillera en collaboration avec la DGS et la DGSIT, au besoin, pour concevoir et mettre en place des solutions pertinentes fondées sur les risques, sur la base des résultats de l'examen de la sécurité. Les procédures internes de la DACT qui seront élaborées à l'issue de la mesure indiquée en 1.1 seront également mises à jour, au besoin, afin de refléter les résultats de l'examen de la sécurité.

Cette mesure sera mise en œuvre au plus tard le 30 décembre 2012.

Recommandation 2 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait vérifier la disponibilité des systèmes de TI classifiés de la DGSMPS afin de s'assurer qu'ils répondent aux besoins opérationnels.

Plan d'action de la gestion 2.1 : La DGSMPS passera en revue les exigences opérationnelles liées à ses systèmes classifiés de TI et en fera part à la DGSIT, au besoin, afin d'assurer le respect de ses besoins opérationnels.

Cette mesure a été réalisée pour la DACT en février 2012 et sera mise en œuvre par la Direction de l'AIPRP au plus tard le 27 avril 2012.

Recommandation 3 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait établir des mesures pour veiller à ce que seules les personnes ayant une autorisation de sécurité appropriée et besoin d'accès afin d'accomplir leurs tâches, aient accès aux systèmes de TI classifiés de la DGSMPS.

Plan d'action de la gestion 3.1 : La DACT et la Direction de l'AIPRP passeront en revue, sur une base trimestrielle, la liste des utilisateurs actifs (rapport de système) tirée de leurs systèmes classifiés de TI afin d'en valider l'autorisation. Ces directions devront par le fait même demander à la DGSIT de valider la liste et les autorisations des employés de la DGSIT qui ont accès à leurs systèmes.

Cette mesure sera mise en œuvre sur une base trimestrielle à compter du 30 avril 2012.

Recommandation 4 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec la sous-ministre adjointe, Direction générale de la surveillance et le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce que les supports électroniques de la DGSMPS, y compris sans s'y limiter, les disques durs d'ordinateur, les clés USB et les disquettes pouvant contenir des renseignements classifiés, soient marqués comme il se doit.

Plan d'action de la gestion 4.1 : La DGSMPS élaborera des procédures afin de veiller à ce que tous les supports électroniques, l'équipement et les appareils pouvant contenir des renseignements classifiés soient identifiés comme il se doit. Ces procédures contiendront également des dispositions portant sur le marquage

adéquat des supports électroniques, de l'équipement et des appareils qui sont hors site et dont la DGSMPS assure le contrôle.

Cette mesure sera mise en œuvre à la DPSAC au plus tard le 31 mai 2012, à la Direction de l'AIPRP d'ici le 29 juin 2012 et à la DACT d'ici le 30 septembre 2012.

Recommandation 5 : La sous-ministre adjointe, Direction générale des services ministériels et des politiques stratégiques (DGSMPS), en collaboration avec le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait veiller à ce qu'une procédure complète et détaillée s'adressant aux personnes devant procéder à l'élimination du matériel pouvant contenir des renseignements classifiés soit élaborée et diffusée.

Plan d'action de la gestion 5.1 : La DGSMPS travaillera en collaboration avec la DGSIT et la DGS, au besoin, afin de passer en revue les lignes directrices en vigueur à l'échelle du Ministère sur l'élimination du matériel électronique et de les modifier, au besoin, de façon à aider les propriétaires ou les organismes gardiens à éliminer le matériel classifié à TPSGC.

Cette mesure sera mise en œuvre au plus tard le 28 septembre 2012.

Plan d'action de la gestion 5.2 : La DGSMPS diffusera les procédures à l'échelle de TPSGC au moyen de communiqués.

Cette mesure sera mise en œuvre au plus tard le 31 octobre 2012.

Recommandation 6 : La sous-ministre adjointe, Direction générale de la surveillance, en collaboration avec le dirigeant principal de l'information, Direction générale des services d'infotechnologie, devrait procéder à une analyse afin de déterminer si les observations et les recommandations de la vérification contenues dans le présent rapport s'appliquent à d'autres unités opérationnelles de TPSGC et, le cas échéant, fournir une orientation fonctionnelle afin de combler les lacunes décelées.

Plan d'action de la gestion 6.1 : Les ministères sont chargés de choisir, de mettre en œuvre et de maintenir des mesures durables de contrôle de la sécurité afin d'atteindre les objectifs établis à ce chapitre. Les contrôles de sécurité peuvent être relatifs à la gestion, de nature administrative, opérationnelle, technique ou procédurale. Les contrôles obligatoires et recommandés sont précisés dans les normes et lignes directrices qui appuient la Politique sur la sécurité du gouvernement. Les ministères peuvent prendre d'autres mesures de contrôle de sécurité et se fixer des objectifs additionnels en se fondant sur les résultats des évaluations des risques. La Directive sur la gestion de la sécurité ministérielle du Conseil du Trésor définit les mesures de contrôle de sécurité qui devraient être comprises dans un programme de sécurité ministérielle efficace.

Examen du Programme de sécurité du Ministère

Le Programme de sécurité du Ministère doit faire l'objet d'un examen exhaustif au moyen des objectifs en matière de contrôle de sécurité établis dans la Directive sur la gestion de la sécurité ministérielle, notamment :

- assurance de l'information;
- enquêtes de sécurité;
- sécurité matérielle;
- sécurité des TI et systèmes de TI;
- sécurité des marchés;
- partage de renseignements et de biens avec d'autres administrations publiques et organisations;
- obtention de services de sécurité auprès d'autres organisations;
- sensibilisation aux questions de sécurité;
- formation sur la sécurité;
- gestion des incidents de sécurité;
- protection des employés contre la violence en milieu de travail,
- inspections de sécurité;
- enquêtes administratives liées aux incidents de sécurité;
- sécurité dans les situations d'urgence et de menace accrue;
- planification des urgences et de la continuité des activités.

L'examen de la sécurité visera les directions générales du Ministère, ainsi que les organismes de service spéciaux et les régions.

Évaluation des menaces et des risques pour l'architecture des activités de programme et profil des risques liés à la sécurité

Une évaluation des menaces et des risques pour l'architecture des activités de programme du Ministère sera réalisée, puisqu'il existe des risques qui pourraient avoir des répercussions sur la capacité de ce dernier d'offrir ses services et d'exécuter ses programmes. L'évaluation fournira une analyse descendante des risques à la sécurité inhérents aux activités de programme du Ministère menées par les directions générales, les organismes de service spéciaux et les régions.

L'examen des programmes et l'évaluation des menaces et des risques seront réalisés conjointement, puisque ces activités sont interreliées.

À PROPOS DE LA VÉRIFICATION

Autorité

La présente vérification a été approuvée par le Comité de vérification et d'évaluation (CVE) de Travaux publics et Services gouvernementaux Canada (TPSGC) dans le cadre du Plan de vérification et d'évaluation axé sur les risques de 2009-2010 à 2013-2014.

Objectif

Cette vérification interne visait à déterminer si certaines directions de la Direction générale des services ministériels et des politiques stratégiques traitaient les renseignements classifiés électroniques conformément à certaines exigences figurant dans des instruments de politique.

Étendue et méthode

La vérification couvrait la période allant de janvier 2009 à avril 2011.

La vérification a permis de déterminer le degré de conformité dans six principaux secteurs d'exigences liés à la création, à l'entreposage, à la transmission et à la destruction des renseignements électroniques classifiés. Elle portait en particulier sur les points suivants :

- le matériel de TI utilisé pour créer et entreposer des renseignements électroniques classifiés;
- la transmission des renseignements électroniques classifiés;
- les autorisations de sécurité des personnes qui traitent les renseignements électroniques classifiés;
- le marquage de sécurité des renseignements électroniques classifiés et des supports de TI;
- la zone de sécurité matérielle dans laquelle les renseignements électroniques classifiés sont traités;
- la destruction ou l'élimination du matériel électronique utilisé pour traiter des renseignements électroniques classifiés.

Trois directions de la Direction générale des services ministériels et des politiques stratégiques ont été sélectionnées pour cette vérification, en raison du risque qu'elles représentent : la Direction des affaires relatives au Conseil du Trésor (DACT), la Direction des politiques stratégiques et des affaires relatives au Cabinet (DPSAC) et la Direction de l'accès à l'information et de la protection des renseignements personnels (AIPRP). Ces directions traitent des renseignements classifiés dans le cadre de la prestation de services au Ministère. Bien que la DACT et la DPSAC aident les agents de TPSGC à rédiger les documents du Cabinet et les présentations au Conseil du Trésor, diverses directions générales au sein de TPSGC sont chargées d'élaborer, de rédiger et d'examiner les mémoires au Cabinet et les présentations au Conseil du Trésor.

L'information ou renseignements de nature délicate est l'information qui doit être protégée, car sa divulgation, son altération, sa perte ou sa destruction pourrait porter préjudice à des biens ou des personnes. Il existe deux types d'information de nature délicate au gouvernement du Canada : les renseignements protégés et les renseignements classifiés. Les renseignements protégés sont les renseignements n'étant pas d'intérêt national. Les catégories de protection sont les suivantes : Protégé A, Protégé B et Protégé C. Les renseignements classifiés correspondent à l'information de nature délicate dont la divulgation non autorisée risquerait vraisemblablement de porter préjudice à l'intérêt national, c'est-à-dire à la sécurité et à la stabilité sociale, politique et économique du Canada. Les catégories de classification sont, par ordre croissant de sensibilité : Confidentiel, Secret et Très secret. La vérification ne comprenait pas l'examen des exigences liées au traitement des renseignements électroniques protégés ou le traitement des renseignements classifiés non électroniques puisque ces secteurs n'étaient pas visés par la vérification. La vérification portait exclusivement sur le traitement des renseignements électroniques classifiés.

La vérification a été réalisée en conformité avec les *Normes internationales pour la pratique professionnelle de la* vérification *interne* de l'Institut des vérificateurs internes.

Pendant la phase d'étude préliminaire, les instruments de politique ont été analysés et des entrevues ont été menées avec les membres de la Direction générale des services ministériels et des politiques stratégiques, de la Direction générale des services d'infotechnologie et du Cabinet du sous-ministre. Une évaluation des risques a été menée et a permis de cerner les risques associés aux exigences définies dans les instruments de politique.

Pendant la phase d'examen, des entrevues approfondies ont été menées auprès du personnel clé travaillant au sein de la DACT, de la DPSAC et de la Direction de l'AIPRP. D'autres entrevues ont été menées auprès d'employés de la DGSIT, en raison de leur rôle de soutien en matière de sécurité des TI et d'administration des systèmes de TI. Les processus et les documents pertinents ont également été examinés et testés. En se fondant sur l'analyse des renseignements et sur les preuves recueillies, l'équipe de vérification a formulé ses constatations et ses conclusions, lesquelles ont été validées auprès des gestionnaires compétents.

Critères

Les critères sont fondés sur une série d'instruments de politique du gouvernement et ont été sélectionnés en fonction du risque. Les instruments de politique utilisés pour déterminer les critères de vérification comprennent :

- La *Politique sur la sécurité du gouvernement*, publiée en 2009 par le Secrétariat du Conseil du Trésor du Canada
- La *Politique sur la sécurité des documents confidentiels du Cabinet* publiée en 2007 par le Bureau du Conseil privé

- Les *Conseils en matière de sécurité des TI (ITSG-06), Écrasement et déclassification des supports d'information électroniques* publié en 2006 par le Centre de la sécurité des télécommunications Canada (CSTC)
- Le *Guide pour l'établissement des zones de sécurité matérielle* publié en 2005 par la Gendarmerie royale du Canada (GRC)
- La *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI), publiée en 2004 par le Secrétariat du Conseil du Trésor du Canada
- La *Norme opérationnelle sur la sécurité matérielle* publiée en 2004 par le Secrétariat du Conseil du Trésor du Canada
- La *Politique ministérielle (PM) 055 - Programme de sécurité de la technologie de l'information.* En juillet 2010, cette politique a été remplacée par la *Politique ministérielle (PM) 104 - Politique sur la sécurité des technologies de l'information.* Étant donné que l'étendue de la vérification chevauchait cette date, les deux politiques ministérielles ont été considérées lors de la vérification.

Les critères étaient les suivants :

- Les renseignements classifiés sont préparés sur des ordinateurs ou des réseaux autonomes appropriés, et des mesures de protection adéquates sont utilisées dans l'entreposage des renseignements.

- Les systèmes utilisés pour traiter les renseignements électroniques classifiés sont certifiés et accrédités selon le niveau de sécurité de l'information qu'ils traitent.

- Des mesures de sécurité appropriées protègent la transmission électronique des renseignements classifiés.

- L'accès aux renseignements classifiés est limité aux personnes qui possèdent l'autorisation de sécurité appropriée.

- Les renseignements électroniques classifiés et les supports de TI utilisés pour entreposer ces renseignements, sont marqués de manière appropriée.

- Les renseignements électroniques classifiés sont préparés et entreposés dans des zones de sécurité matérielle appropriées.

- L'équipement de TI qui renferme des renseignements électroniques classifiés est détruit ou éliminé selon des méthodes et des procédures appropriées.

Fin des travaux de vérification

Les travaux menés aux fins de cette vérification ont essentiellement été terminés le 30 avril 2011.

Équipe de vérification

La vérification a été menée par le personnel du Bureau de la vérification et de l'évaluation ainsi que par un expert-conseil en vérification, sous la supervision du directeur, Direction des services de la vérification interne, et sous la direction générale de la Dirigeante principale de la vérification et de l'évaluation.

La vérification a été revue par la fonction de l'Examen de la qualité du Bureau de la vérification et de l'évaluation**.**