Secrétariat du Conseil du Trésor du Canada
Treasury Board of Canada Secretariat
Canada

Politique sur la sécurité du gouvernement

Publié : le 01 avr. 2012

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

N° de catalogue BT39-22/2012F-PDF
ISBN : 978-0-660-09915-6

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Policy on Government Security

Politique sur la sécurité du gouvernement

1. Date d'entrée en vigueur

1.1 La présente politique entre en vigueur le 1er juillet 2009.

1.2 Cette version de la politique renferme des mises-à-jour qui prennent effet le 1er avril 2012.

2. Application

2.1 La présente politique s'applique :

- à tous les ministères mentionnés aux annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP), sauf s'ils en sont exclus en vertu d'une loi, d'un règlement ou d'un décret particulier.

3. Contexte

3.1 La sécurité du gouvernement, c'est l'assurance que l'information, les biens et les services ne sont pas compromis et que les personnes sont protégées contre la violence en milieu de travail. La mesure dans laquelle le gouvernement peut assurer sa propre sécurité influe directement sur sa capacité de garantir que les services qui contribuent à la santé, à la sécurité et au mieux-être économique des Canadiennes et des Canadiens continuent d'être fournis.

3.2 La sécurité commence en établissant une confiance dans les interactions impliquant le gouvernement et les Canadiens ainsi que dans celles prenant place au sein du gouvernement lui-même. Dans ses interactions avec la population, comme requise, le gouvernement a besoin de connaître l'identité de la personne ou de l'institution avec laquelle il transige. Au sein du gouvernement, il est nécessaire de veiller à ce que les personnes qui ont accès aux renseignements, aux biens et aux services gouvernementaux soient dignes de confiance, fiables et loyales. Ainsi, un large éventail d'activités gouvernementales, qu'il s'agisse de protéger l'information et les biens, de fournir des services, des prestations ou des indemnités, ou encore d'intervenir en cas d'incident ou d'urgence, reposent sur ce lien de confiance.

3.3 Dans un ministère, la gestion de la sécurité exige une évaluation continue des risques ainsi que la mise en place, la surveillance et le maintien de mécanismes appropriés de contrôle de gestion interne en matière de prévention (atténuation), de détection, d'intervention ou de rétablissement. La gestion de la sécurité recoupe d'autres fonctions de gestion, dont l'accès à l'information, la protection des renseignements personnels, la gestion du risque, la gestion des urgences et de la poursuite des activités, la gestion des ressources humaines, la santé et la sécurité au travail, l'immobilier, la gestion du matériel, la gestion de l'information, les technologies de l'information (TI) et les finances. La sécurité est assurée lorsqu'elle est appuyée par la haute direction, une dimension qui fait partie intégrante de la planification stratégique et opérationnelle, et qu'elle est intégrée aux cadres, à la culture et aux activités courantes des ministères ainsi qu'aux comportements des employés.

3.4 À l'échelle d'un gouvernement, il faut gérer les menaces à la sécurité, les risques et les incidents de façon proactive pour faciliter la protection des biens, des renseignements et des services critiques du gouvernement, et assurer, dans le même temps, la sécurité nationale. Les conseils, l'orientation et les services que fournissent les principaux organismes responsables de la sécurité aident les ministères et le gouvernement à maintenir des niveaux acceptables de sécurité tout en réalisant les objectifs stratégiques et en satisfaisant aux impératifs liés à la prestation de services.

3.5 La gestion de la sécurité est la plus efficace lorsqu'elle fait partie intégrante des activités, des programmes et de la culture d'un ministère et de la fonction publique dans son ensemble.

3.6 Les administrateurs généraux sont responsables de la mise en œuvre et de l'administration efficace de la gestion de la sécurité et de l'identité au sein de leur ministère, et ils partagent la responsabilité d'assurer la sécurité du gouvernement dans son ensemble. Ces responsabilités englobent la sécurité du personnel ministériel, y compris des personnes qui travaillent dans les cabinets de ministres ou de ministres d'État, ou pour ceux-ci, ainsi que des renseignements, des installations et des autres biens des ministères.

3.7 Les ministres d'État, ministres et ministres d'État sont responsables de la sécurité de leur personnel et de leurs bureaux ainsi que de la sécurité des renseignements et des biens de nature délicate dont ils ont la garde, conformément aux directives du premier ministre.

3.8 La présente politique est émise en vertu de l'article 7 de la LGFP.

3.9 Le Conseil du Trésor a délégué au Président du Conseil du Trésor le pouvoir de modifier les directives qui appuient la politique dans les domaines suivants :

- la gestion de la sécurité ministérielle;
- la gestion de l'identité;

et de diffuser et de modifier les normes qui appuient la politique dans les domaines suivants :

- l'assurance de l'information et de l'identité;
- les enquêtes de sécurité;

- la sécurité matérielle;
- la sécurité des TI;
- la gestion des urgences et de la continuité des activités;
- la sécurité des marchés.

3.10 La présente politique doit être lue en parallèle avec le *Cadre principal des politiques du Conseil du Trésor,* la *Directive sur la gestion de la sécurité ministérielle*, et la *Directive sur la gestion de l'identité.*

4. Définitions

4.1 Les définitions relatives aux termes utilisés dans la présente politique se trouvent à l'annexe A – Définitions.

5. Énoncé de la politique

5.1 La présente politique a pour objectif de veiller à ce que les administrateurs généraux gèrent efficacement les activités de sécurité au sein des ministères et contribuent à la gestion efficace de la sécurité à l'échelle du gouvernement.

5.2 Les résultats escomptés de la présente politique sont les suivants :

- l'information, les biens et les services ne sont pas compromis et les employés sont protégés contre la violence en milieu de travail;
- les structures, mécanismes et ressources de gouvernance sont en place pour assurer la gestion efficace et efficiente de la sécurité, tant au sein d'un ministère que dans l'ensemble du gouvernement;
- la gestion des incidents de sécurité est efficacement coordonnée au sein des ministères et dans l'ensemble du gouvernement;
- l'interopérabilité et l'échange de renseignements sont assurés au moyen de pratiques efficaces et uniformes en matière de gestion de la sécurité et de l'identité;
- la continuité des activités et des services du gouvernement est assurée en cas d'incidents de la sécurité, de perturbations ou de situations d'urgence.

6. Exigences

6.1 Les administrateurs généraux de tous les ministères sont responsables de ce qui suit :

6.1.1 Mettre sur pied un programme de sécurité afin d'assurer la coordination et la gestion des activités ministérielles liées à la sécurité qui :

a. repose sur une structure de gouvernance assortie de responsabilités claires;
b. comporte des objectifs précis qui cadrent avec les politiques, les priorités et les plans ministériels et pangouvernementaux;
c. est suivi, évalué et fait l'objet de rapports afin de mesurer les efforts, les ressources et les réussites de la direction à l'égard de l'atteinte des résultats escomptés;

6.1.2 Nommer un agent de sécurité du ministère (ASM) relevant de l'administrateur général ou du comité exécutif ministériel pour gérer le programme de sécurité du ministère (Nota : l'administrateur général d'un petit ministère ou organisme (PMO) peut occuper le rôle de l'ASM);

6.1.3 Prendre un arrangement formel avec le fournisseur de services quand le rôle de l'ASM est occupé par un tiers (p. ex., un fournisseur de services partagés ou regroupés ou un ministère responsable du portefeuille).

6.1.4 Approuver le programme de sécurité ministérielle qui détaille les décisions en matière de gestion de risques liés à la sécurité et expose les stratégies, les buts, les objectifs et les échéanciers élaborés en vue d'améliorer la sécurité ministérielle et de favoriser sa mise en œuvre;

6.1.5 S'assurer que les gestionnaires de tous niveaux intègrent les exigences relatives à la gestion de la sécurité et de l'identité aux plans, aux programmes, aux activités et aux services;

6.1.6 Veiller à ce que toutes les personnes qui auront accès aux renseignements et aux biens du gouvernement, y compris les personnes qui travaillent dans les cabinets de ministres ou de ministres d'État ou pour ceux-ci, fassent l'objet d'une enquête de sécurité appropriée avant de commencer leur travail et soient traitées de manière juste et impartiale;

6.1.7 Veiller à ce que leur pouvoir de refuser, de révoquer ou de suspendre les autorisations de sécurité ne soit pas délégué;

6.1.8 S'assurer que les enjeux importants concernant la conformité à la politique, les allégations d'inconduite, les activités criminelles soupçonnées, les incidents liés à la sécurité ou la violence en milieu de travail fassent l'objet d'une enquête, d'une intervention et d'un signalement à l'organisme approprié chargé de l'application de la loi, à l'organisme de sécurité nationale ou à l'organisme principal responsable de la sécurité;

6.2 Les administrateurs généraux des principaux organismes responsables de la sécurité sont responsables de ce qui suit :

6.2.1 Fournir aux ministères des conseils, de l'orientation et des services liés à la sécurité du gouvernement, conformément aux responsabilités qui leur sont confiées;

6.2.2 Nommer un ou plusieurs cadres qui seront chargés de coordonner et de superviser la prestation de services de soutien aux

ministères et de représenter l'administrateur général auprès du SCT à cet égard;

6.2.3 Veiller à ce que les services de soutien à la sécurité qui sont fournis aident les ministères à atteindre et à maintenir un état acceptable de sécurité et de préparation et à ce que ces services concordent toujours avec les politiques, priorités et plans pangouvernementaux ayant trait à la sécurité du gouvernement;

- L'annexe B – Responsabilités des principaux organismes responsables de la sécurité, dresse une liste des principaux organismes responsables de la sécurité et fournit des précisions sur la nature et la portée de leurs responsabilités aux termes de la présente politique.

6.3 Surveillance et déclaration

Au sein des ministères

- Les administrateurs généraux doivent veiller à ce que l'on procède à des examens périodiques pour déterminer si le programme de sécurité ministérielle est efficace, si les buts, les objectifs stratégiques et les objectifs de contrôle précisés dans leur plan de sécurité ministérielle ont été atteints, et si ce plan continue de répondre aux besoins du ministère et du gouvernement dans son ensemble.

Par les ministères

- Les administrateurs généraux doivent faire rapport périodiquement au SCT sur la situation et l'état d'avancement de la mise en œuvre de la présente politique et sur les résultats concernant la mesure continue du rendement.

Principaux organismes responsables de la sécurité

- En plus de surveiller leur programme de sécurité ministérielle et d'en rendre compte, les administrateurs généraux des principaux organismes responsables de la sécurité sont également responsables de ce qui suit :
- s'assurer que l'on procède à des examens périodiques en vue d'évaluer l'efficacité de leurs services de soutien à la sécurité afin de veiller à ce que ces services continuent de répondre aux besoins des ministères et du gouvernement dans son ensemble;
- rendre compte des activités qu'ils mènent en vertu de la présente politique, au moyen des mécanismes actuels de rapport du gouvernement, comme la Structure de gestion des ressources et des résultats, les rapports ministériels sur le rendement (RMR) et les rapports sur les plans et les priorités (RPP).

À l'échelle du gouvernement

- Le SCT est responsable de ce qui suit :
    - surveiller la conformité à la présente politique et l'atteinte des résultats escomptés de diverses manières, y compris, sans s'y limiter, au moyen d'évaluations fondées sur le Cadre de responsabilisation de gestion, de présentations au Conseil du Trésor, des RMR, des RPP, des résultats des vérifications, des évaluations et des études, ainsi qu'au moyen du dialogue continu et des travaux des comités;
    - examiner l'efficacité et la mise en œuvre de la présente politique ainsi que de ses directives et normes cinq ans après la date d'entrée en vigueur de la politique, et en rendre compte au Conseil du Trésor. Si une analyse des risques le justifie, le SCT veillera aussi à ce qu'une évaluation soit réalisée.

7. Conséquences

7.1 L'administrateur général est chargé de veiller à ce que des mesures correctives appropriées soient prises pour traiter des questions concernant la conformité à la politique, les allégations d'inconduite, les activités criminelles soupçonnées ou les incidents de sécurité, notamment en refusant, en révoquant ou en suspendant les autorisations de sécurité et de fiabilité, selon le cas.

7.2 Si le secrétaire du Conseil du Trésor détermine qu'un ministère peut avoir dérogé à l'une des exigences de la présente politique ou de ses directives ou normes connexes, il peut demander à l'administrateur général de ce ministère :

7.2.1 de procéder à une vérification ou à un examen, dont le coût sera imputé au niveau de référence du ministère, pour déterminer si les exigences de la présente politique ou de ses directives à l'appui ont été satisfaites;

7.2.2 de prendre des mesures correctives et de rendre compte des résultats.

7.2.3 L'inobservation de la présente politique et de ses directives et normes à l'appui ou le défaut de prendre les mesures correctives demandées par le secrétaire du Conseil du Trésor peut donner lieu à diverses conséquences, notamment de recommander au Conseil du Trésor d'imposer d'autres mesures jugées appropriées dans les circonstances.

8. Références

Les documents suivants sont pertinents aux fins de la présente politique :

- *Charte canadienne des droits et libertés*
- *Code canadien du travail*
- *Code criminel*
- *Loi canadienne sur les droits de la personne*

- *Loi d'interprétation*
- *Loi sur l'emploi dans la fonction publique*
- *Loi sur la Bibliothèque et les Archives du Canada*
- *Loi sur la défense nationale*
- *Loi sur la Gendarmerie royale du Canada*
- *Loi sur la gestion des finances publiques*
- *Loi sur la gestion des urgences*
- *Loi sur la preuve au Canada*
- *Loi sur la production de défense*
- *Loi sur la protection de l'information*
- *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*
- *Loi sur la protection des renseignements personnels*
- *Loi sur la statistique*
- *Loi sur l'accès à l'information*
- *Loi sur le casier judiciaire*
- *Loi sur le ministère des Affaires étrangères et du Commerce international*
- *Loi sur le service canadien du renseignement de sécurité*
- *Loi sur le système de justice pénale pour les adolescents*
- *Loi sur les immeubles fédéraux et les biens réels fédéraux*
- *Loi sur les relations de travail dans la fonction publique*
- *Règlement canadien sur la santé et la sécurité au travail*

Les politiques, directives et normes suivantes du Conseil du Trésor sont pertinentes aux fins de la présente politique :

- *Cadre de gestion intégrée du risque*
- *Cadre de politiques en matière de langues officielles*
- *Cadre de politique sur la gestion des actifs et services acquis*
- *Cadre des politiques de gestion de la rémunération*
- *Cadre principal des politiques du Conseil*
- *Cadre stratégique pour l'information et la technologie*
- *Code de valeurs et d'éthique de la fonction publique*
- *Directive sur la gestion de l'identité*
- *Directive sur la gestion de la sécurité ministérielle*
- *Directive sur les marchandises contrôlées*
- *Directive sur les rôles et responsabilités en matière de gestion de l'information*
- *Norme de sécurité et de gestion des marchés*
- *Norme de sécurité opérationnelle – Programme de planification de la continuité des activités (PCA)*
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI)*
- *Norme opérationnelle sur la sécurité matérielle*
- *Norme sur la sécurité du personnel*
- *Politique de communication du gouvernement du Canada*
- *Politique en matière d'apprentissage, de formation et de perfectionnement*
- *Politique sur l'accès à l'information*
- *Politique sur l'évaluation*
- *Politique sur la gestion de l'information*
- *Politique sur la gestion des biens immobiliers*
- *Politique sur la gestion des projets*
- *Politique sur la gestion des risques*
- *Politique sur la gestion des technologies de l'information*
- *Politique sur la gestion du matériel*
- *Politique sur la protection contre les incendies, enquêtes et rapports*
- *Politique sur la protection de la vie privée*
- *Politique sur la structure de la gestion, des ressources et des résultats*
- *Politique sur la vérification interne*
- *Politique sur les contrôles internes*
- *Politique sur les langues officielles pour la gestion des ressources humaines*
- *Politique sur les marchés*
- *Politique sur les pertes de deniers et infractions et autres actes illégaux commis contre la Couronne*
- *Politique sur les plans d'investissement à long terme*
- *Programme de coordination de l'image de marque*
- *Sécurité et la santé au travail*

9. Demandes de renseignements

Veuillez adresser toute demande de renseignements au sujet de la présente politique à votre ASM. Pour obtenir de l'aide au sujet de l'interprétation de la présente politique, l'ASM doit communiquer avec :

Division de la sécurité et gestion de l'identité

Direction du dirigeant principal de l'information
Secrétariat du Conseil du Trésor
Ottawa ON K1A 0R5

Courriel : SIDM-SGID@tbs-sct.gc.ca
Téléphone : (613) 946-5046
Télécopieur : (613) 952-7232
Téléscripteur : (613) 957-9090 (SCT)

Annexe A – Définitions

Administrateur général (*Deputy Head*)
: Administrateur général tel que défini à l'article 11 de la *Loi sur la gestion des finances publiques* et, dans le cas des Forces canadiennes, le chef d'état-major de la Défense.

cadre supérieur (*executive*)
: Employé nommé au niveau du groupe de la direction (niveaux EX-01 à EX-05), c.-à-d. un directeur, un directeur général, un sous-ministre adjoint ou l'équivalent.

compromission (*compromise*)
: Accès, divulgation, destruction, suppression, modification, utilisation ou interruption non autorisés de biens ou de renseignements.

confidentialité (*confidentiality*)
: Qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées, afin de prévenir tout préjudice à l'intérêt national ou à d'autres intérêts.

connaissance de la situation (*situational awareness*)
: Avoir une compréhension de son environnement et de ce qui se passe pour comprendre comment les événements et les mesures influeront sur les objectifs opérationnels, maintenant et dans un proche avenir. Il est essentiel de bien connaître la situation, de manière précise, actualisée et complète dans tout domaine où la complexité technologique, le processus décisionnel et le bien-être du public interagissent. Comme la gestion des incidents fait intervenir des prédictions et des prévisions, il est essentiel, pour connaître la situation d'un domaine de la TI, de saisir les relations qui existent entre les services et les renseignements essentiels, les mécanismes de protection de l'infrastructure et des processus de TI, de même que l'évolution des menaces.

contrôle de sécurité (*security control*)
: Mesure administrative, opérationnelle, technique, physique ou juridique visant à gérer les risques pour la sécurité. Cette expression est synonyme de protection.

cote de fiabilité (*reliability status*)
: Indique que l'évaluation de fiabilité a été complétée avec succès et donne à la personne visée un accès régulier aux biens gouvernementaux et un accès à des renseignements PROTÉGÉS en fonction du besoin de connaître.

cote de sécurité (*security clearance*)
: Indique que l'évaluation de sécurité a été complétée avec succès; avec un besoin de connaître, permet d'avoir accès à des renseignements classifiés. Il y a trois niveaux : confidentiel, secret et très secret.

disponibilité (*availability*)
: Condition d'être accessible et utilisable de manière fiable et en temps opportun.

enquête de sécurité (*security screening*)
: Toute mesure permettant d'obtenir un degré élevé d'assurance qu'une personne peut se voir accorder des privilèges d'accès spécifiques au sein du gouvernement fédéral.

gestion de l'identité (*identity management*)
: Ensemble de principes, de pratiques, de processus et de procédures permettant de remplir le mandat d'une organisation et d'atteindre ses objectifs liés à l'identité.

gestion des urgences (*emergency management*)
: La prévention et l'atténuation des situations d'urgence, la préparation et de la réaction à ces situations ainsi que le rétablissement des activités.

identité (*identity*)
: Référence ou désignation utilisée pour distinguer une personne, une organisation ou un appareil unique et particulier.

incident complexe de sécurité des TI (*sophisticated IT security incident*)
: Événement habituellement déclenché par les auteurs d'une menace complexe qui est compliqué à détecter, dont il est difficile de se remettre, qui cause un préjudice aux réseaux et systèmes du gouvernement du Canada et qui porte atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information.

incident de sécurité (*security incident*)
: Tout acte de violence en milieu de travail manifestée à l'endroit d'un employé ou tout acte, événement ou omission pouvant entraîner la compromission d'informations, de biens ou de services.

intérêt national (*national interest*)
: La sécurité du Canada ainsi que sa stabilité sociale, politique et économique.

interopérabilité (*interoperability*)
: Capacité des ministères du gouvernement fédéral de fonctionner en synergie au moyen de pratiques uniformes en matière de gestion de la sécurité et de l'identité.

menace (*threat*)
: Événement ou acte délibéré ou accidentel qui pourrait porter préjudice aux personnes, à l'information, aux biens ou aux services.

menace complexe à la sécurité des TI (*sophisticated IT security threat*)
Entité qui recourt à des technologies de pointe et à des procédés perfectionnés pour pénétrer ou contourner des systèmes de protection et des technologies de sécurité sans être décelée.

ministère (*department*)
Les ministères mentionnés à l'annexe I, les divisions ou directions de l'administration publique fédérale mentionnées à la colonne I de l'annexe I, et les secteurs de l'administration publique fédérale mentionnés aux annexes IV et V de la Loi sur la gestion des finances publiques (LGFP), sauf s'ils en sont exclus en vertu d'une loi, d'un règlement ou d'un décret particulier.

planification de la continuité des activités (*business continuity planning*)
Élaboration et exécution en temps opportun de plans, de mesures, de procédures et de dispositions afin d'éviter ou de minimiser toute interruption de la disponibilité des services et des biens essentiels.

renseignement électromagnétique (SIGINT) (*Signals intelligence (SIGINT)*)

Information technique ou renseignement comportant (seul ou en combinaison) du renseignement sur les communications (COMINT), du renseignement électronique (ELINT) et du renseignement tiré de signaux d'instrumentation étrangers (FISINT).

renseignement électronique (*ELINT*)
Information technique ou renseignement tiré de la collecte, du traitement et de l'analyse d'émissions électromagnétiques autres que de communications.

renseignement tiré de signaux d'instrumentation étrangers (*FISINT*)
Information technique ou renseignement tiré de la collecte, du traitement et de l'analyse de signaux d'instrumentation étrangers par une personne autre que le destinataire prévu.

renseignement sur les communications (*COMINT*)
Information technique ou renseignement tiré de l'exploitation, par une personne autre que le destinataire prévu, de systèmes de télécommunications, de systèmes et de réseaux de technologie de l'information, ainsi que de toute donnée ou information technique véhiculée par ceux-ci, contenue dans ceux-ci ou s'y rapportant.

risque (*risk*)
Incertitude que peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation.

sécurité des communications (COMSEC) (*Communications Security (COMSEC)*)
Application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions et de sécurité matérielle ainsi que de pratiques et de mécanismes de contrôle opérationnels pour empêcher tout accès non autorisé à l'information issue de télécommunications et pour garantir l'authenticité de ces télécommunications.

service essentiel (*critical service*)
Service dont la compromission, du point de vue de la disponibilité ou de l'intégrité, porterait un grave préjudice à la santé, à la sûreté, à la sécurité ou au bien-être économique des Canadiens, ou encore au fonctionnement efficace du gouvernement du Canada.

urgence (*emergency*)
Événement présent ou imminent, y compris les incidents liés aux technologies de l'information, nécessitant des actions rapides et coordonnées pour protéger la santé, la sécurité ou le bien-être de personnes ou encore pour limiter les dommages à des biens ou à l'environnement.

violence en milieu de travail (*workplace violence*)
Agissement, conduite, menace ou geste qui pourrait vraisemblablement causer un dommage, des blessures ou une maladie à un employé en milieu de travail.

vulnérabilité (*vulnerability*)
Insuffisance liée à la sécurité qui pourrait accroître la susceptibilité à la compromission ou au préjudice.

Annexe B – Responsabilités des principaux organismes responsables de la sécurité

Les principaux organismes responsables de la sécurité fournissent conseils, orientation et services pour appuyer les opérations courantes de sécurité des ministères et permettre au gouvernement dans son ensemble de gérer efficacement les activités de sécurité, de coordonner les interventions en cas d'incidents de sécurité et d'atteindre et de maintenir un état acceptable de sécurité et de préparation. La présente annexe décrit les responsabilités de ces organismes relativement à leurs champs ou domaines d'expertise.

Le **Secrétariat du Conseil du Trésor (SCT)** établit et supervise une approche pangouvernementale de gestion de la sécurité et de l'identité, en tant qu'élément clé de toutes les activités de gestion, et surveille si les services sont suffisants pour soutenir ces activités et pratiques dans l'ensemble du gouvernement. Le SCT est responsable de ce qui suit :

- établir et maintenir un régime de gouvernance de la sécurité interministérielle pour assurer une supervision stratégique de la sécurité du gouvernement, et assumer la direction et recommander les priorités relatives :
    - aux politiques du gouvernement sur la sécurité et aux approches en matière de développement d'une collectivité de la sécurité;
    - à l'établissement de normes et à la désignation des autorités nécessaires pour identifier et authentifier les personnes, à l'intérieur et à l'extérieur du gouvernement du Canada;
    - aux services de sécurité fournis par les principaux organismes responsables de la sécurité;
    - à la gestion des incidents (y compris les activités de préparation, d'atténuation, d'intervention, de reprise et d'analyse postérieure à l'incident ayant trait à la sécurité;
- établir une orientation pangouvernementale, fixer des priorités et définir et officialiser des exigences en matière de gestion de

la sécurité et de l'identité pour le gouvernement du Canada et les ministères;
- établir une orientation pangouvernementale et définir les exigences relatives au CIDP et au NIO.
- orienter les principaux organismes responsables de la sécurité à l'égard des stratégies de formation et de sensibilisation et coordonner des programmes de formation et de sensibilisation pour le développement ou le perfectionnement des collectivités de la sécurité et de l'identité, des praticiens de la sécurité, des gestionnaires de tous niveaux et d'autres collectivités fonctionnelles;
- établir et diriger les forums et événements concernant les collectivités de la sécurité et de l'identité pour assister les ministères dans la mise en œuvre de la *Politique sur la sécurité du gouvernement*;
- en collaboration avec les principaux organismes responsables de la sécurité, fixer des normes de service en matière de prestation de conseils, de directives et de services à l'appui de la mise en œuvre de la *Politique sur la sécurité du gouvernement* et surveiller les progrès en vue de l'atteinte des résultats souhaités;
- entretenir des liens étroits avec Sécurité publique Canada, surveiller et évaluer ses produits d'information pour cerner les incidents pouvant avoir des répercussions sur le service public et formuler des recommandations au sujet de la mise en œuvre des plans d'intervention en cas d'urgence et d'incident;
- fournir orientation et conseils aux principaux organismes responsables de la sécurité et aux ministères au sujet de l'approche à adopter et des mesures à mettre en œuvre pour gérer les incidents de sécurité, y compris les incidents touchant à la sécurité du gouvernement, à l'exploitation des réseaux et systèmes de TI du gouvernement, à la prestation des services et à la confiance dans le gouvernement;
- surveiller la gestion des incidents afin d'assurer que les objectifs stratégiques du gouvernement sont maintenus. Cela comprend, sans s'y limiter, la réalisation d'examens rétrospectifs des activités de gestion des incidents, le suivi des rapports d'intervention après incident et l'élaboration des leçons apprises.

Le **Bureau du Conseil privé (BCP)** conseille et appuie le premier ministre et le Cabinet sur les questions de sécurité nationale et coordonne les activités connexes des ministères et organismes. Le BCP est responsable de ce qui suit :

- fournir une orientation stratégique pangouvernementale sur les priorités en matière de sécurité nationale et de renseignement;
- conseiller les ministères sur les stratégies, activités et mécanismes nécessaires pour élaborer, mettre en œuvre, évaluer et améliorer un système de sécurité complètement intégré au sein du gouvernement du Canada, à l'appui des objectifs de sécurité nationale;
- fournir des directives à Sécurité publique Canada pour contribuer à résoudre les incidents de sécurité du gouvernement et les événements susceptibles d'avoir une incidence sur la sécurité nationale;
- fournir des directives et des conseils aux ministères et organismes sur la mise en œuvre des niveaux de sécurité appropriés dans les situations d'urgence et de menace accrues;
- aider le premier ministre à déterminer si des candidats sont aptes à occuper des charges publiques, et effectuer des vérifications de sécurité pour les administrateurs généraux;
- fournir des directives et des conseils aux ministères et organismes sur le niveau de soutien à la sécurité devant être procuré aux ministres, aux secrétaires d'État et aux secrétaires parlementaires;
- établir une politique gouvernementale sur la sécurité des documents confidentiels du Cabinet (documents confidentiels du Conseil privé de la Reine pour le Canada) et des documents gérés dans le cadre du Système des dossiers du Cabinet, et coordonner les enquêtes menées sur les cas de divulgation non autorisée ou de compromission de ces documents.

Sécurité publique Canada (SPC) coordonne les activités liées aux urgences (lesquelles comprennent les incidents de TI) qui touchent le gouvernement du Canada et assume la direction dans le domaine de la gestion des urgences, ce qui comprend la continuité des activités et la gestion des incidents de TI. SPC est responsable de ce qui suit :

- établir des politiques, des normes et des programmes relatifs à la gestion des urgences;
- fournir conseils et orientation aux ministères à l'égard du développement d'une connaissance de la situation grâce à l'identification des renseignements, des biens et des installations qui appuient les services critiques et les opérations gouvernementales, et définir les rapports de dépendance et d'interdépendance entre ces activités, afin :
    - d'aider à accroître l'état de préparation du gouvernement et de renforcer sa capacité d'intervention;
    - de gérer les situations d'urgence;
    - d'appuyer le processus décisionnel fédéral;
- fournir des conseils et de l'orientation aux ministères à l'égard de la préparation, du maintien, de la mise à l'essai et de la mise en œuvre des plans de gestion des urgences et de continuité des activités;
- assurer la coordination centrale pour évaluer les nouvelles menaces complexes et pour élaborer et promouvoir des approches détaillées et coordonnées afin de tenir compte des risques au sein du gouvernement fédéral et à l'échelle du Canada;
- concevoir et mettre en œuvre des programmes et stratégies d'apprentissage et de formation en gestion des urgences à l'intention des collectivités fédérales;
- partager les leçons apprises et les pratiques exemplaires avec les praticiens de la gestion des urgences et faciliter le partage de l'information au sein du gouvernement du Canada, et entre le gouvernement du Canada et ses partenaires pertinents;
- coordonner l'élaboration d'exercices nationaux et régionaux de gestion des urgences et donner aux ministères des conseils à ce sujet;
- favoriser la connaissance des questions relatives à la gestion des urgences et faciliter le partage de l'information pour améliorer la gestion des urgences et des incidents;
- fournir de l'information, des conseils et de l'orientation au gouvernement du Canada sur la gestion des urgences;
- représenter le gouvernement du Canada dans le cadre d'initiatives régionales, nationales, et internationales liées à la gestion des urgences;
- communiquer les décisions du BCP qui exigent des ministères et organismes qu'ils mettent en œuvre un niveau de préparation en réaction aux menaces à la sécurité;
- surveiller les situations d'urgence potentielles, imminentes et actuelles, y compris celles qui ont d'importantes répercussions sur les TI, conseiller les autres ministères et le SCT en conséquence et coordonner la gestion des urgences qui influent ou peuvent influer sur les services aux Canadiens, sur les opérations gouvernementales ou sur le fonctionnement efficace du

gouvernement. À ce titre, SPC est responsable de ce qui suit :

- surveiller les menaces aux services à la population canadienne, aux opérations gouvernementales ou au fonctionnement efficace du gouvernement, y compris sans s'y limiter aux réseaux, systèmes d'information et autres infrastructures essentielles du gouvernement, fournir aux ministères des conseils, de l'orientation et des rapports portant sur la connaissance de la situation relativement à des situations d'urgence potentielles ou réelles, et coordonner la réaction du gouvernement du Canada à cet égard et la reprise des activités après une urgence;
- donner suite aux demandes émanant des ministères gouvernementaux en quête de conseils techniques particuliers, d'orientation et d'information sur les interventions et la reprise des activités à la suite d'incidents de TI;
- réaliser des analyses postérieures à l'incident et rédiger des rapports postérieurs aux mesures prises, et recommander au SCT et aux ministères des mesures visant à réduire le risque d'incidents semblables à l'avenir; et
- faire rapport au SCT pendant toutes les étapes de la gestion de l'incident, y compris produire son analyse des événements et incidents qui ont influé ou ont pu influer sur les services à la population canadienne, sur les opérations gouvernementales ou sur le fonctionnement efficace du gouvernement.

Le **Centre de la sécurité des télécommunications du Canada (CSTC)** assure la direction et la coordination des activités ministérielles en vue de protéger les renseignements électroniques et les systèmes d'information d'importance, et agit à titre d'autorité nationale du gouvernement pour les renseignements électromagnétiques (SIGINT) et la sécurité des télécommunications (COMSEC). Le CSTC est responsable de ce qui suit :

- élaborer, en fonction d'une analyse des besoins de la collectivité et en collaboration avec le SCT, des instruments de politique ayant trait à la sécurité des TI aux fins d'approbation par le SCT;
- élaborer, approuver et promulguer des instruments de politique liés à la COMSEC et aux SIGINT à l'égard des renseignements classifiés, et concevoir des lignes directrices et des outils s'appliquant à la sécurité des TI;
- coordonner l'élaboration et la prestation d'activités de formation et de sensibilisation liées à la sécurité des TI, à la COMSEC et aux SIGINT, à l'intention des agents de sécurité des ministères, des praticiens de la sécurité et, au besoin, d'autres personnes autorisées;
- diriger des groupes de travail et des comités interministériels responsables de la sécurité des TI et faciliter le partage de l'information et la collaboration entre les collectivités de la sécurité;
- recueillir et examiner les pratiques exemplaires en matière de sécurité des TI et formuler des recommandations au SCT et aux comités de gouvernance de la sécurité pour faciliter les améliorations à la politique sur la sécurité ainsi que la collaboration entre les ministères;
- effectuer des recherches sur les méthodes, technologies et services communs liés à la sécurité des TI et proposer des solutions au SCT et aux comités de gouvernance afin d'améliorer la gestion des risques et de réaliser des économies d'échelle au sein du gouvernement;
- autoriser des cours spéciaux d'initiation aux SIGINT et tenir un inventaire national du personnel autorisé et initié aux SIGINT;
- autoriser l'exploitation des systèmes et installations de TI qui gèrent des renseignements électromagnétiques;
- réagir et participer aux enquêtes ou aux analyses portant sur des incidents complexes de sécurité des TI, ainsi que sur des menaces et des vulnérabilités à cet égard, et donner suite aux renseignements recueillis ou reçus à l'issue de ces enquêtes;
- conseiller et orienter les ministères :
    - sur la protection et la diffusion des SIGINT,
    - sur l'utilisation et la mise en application des produits de sécurité des TI, des dispositifs de la COMSEC, des mesures cryptographiques et de la gestion des clés,
    - sur la certification des services partagés et communs de TI, sur les nouvelles technologies de sécurité des TI, sur la conception de l'architecture de la sécurité des TI, sur les solutions communes de sécurité des TI, y compris l'utilisation sécuritaire des produits commerciaux, sur la conception de dispositifs de sécurité pour les systèmes et réseaux ainsi que sur les évaluations de la posture de sécurité et de la vulnérabilité,
    - sur la conception et la mise à niveau des infrastructures de TI du gouvernement du Canada et de leurs interconnectivités de sécurité,
    - sur l'application des dispositifs de contrôle d'accès aux TI à des fins de confidentialité et d'intégrité ainsi que de détection des menaces et de prévention,
    - sur la certification des services de TI partagés, communs ou fédérés du gouvernement du Canada;
- offrir des services aux ministères pour :
    - les systèmes de gestion des clés et leurs composantes connexes aux fins du traitement des renseignements classifiés,
    - la prédiction et la prévention des incidents complexes de sécurité des TI et les menaces et vulnérabilités à cet égard, de même que la protection contre ces incidents, menaces et vulnérabilités,
    - la prise en compte et l'atténuation des risques d'incidents complexes de sécurité des TI,
    - la conception d'architecture de sécurité pour les initiatives partagées, communes ou fédérées du gouvernement du Canada,
    - l'évaluation des produits de sécurité des TI ou l'approbation des produits en usage dans le domaine des renseignements classifiés, lorsqu'on le juge nécessaire,
    - le soutien technique et opérationnel adapté à l'égard des projets d'infrastructure d'information qui revêtent de l'importance pour le gouvernement du Canada,
    - la certification et l'accréditation des systèmes et installations de TI pour le traitement des SIGINT;
- élaborer, en collaboration avec Travaux publics et Services gouvernementaux Canada, des mécanismes d'acquisition de produits et de services préapprouvés de sécurité des TI;
- recueillir et analyser les renseignements regroupés sur les menaces à la sécurité des TI et la vulnérabilité à cet égard, et en faciliter le partage autorisé avec les ministères et SPC;
- représenter le gouvernement du Canada dans le cadre d'initiatives nationales et internationales portant sur la sécurité des TI et sur les SIGINT.

Travaux publics et Services gouvernementaux Canada (TPSGC) assure la direction et la coordination des activités

ministérielles facilitant l'application de mesures de sécurité à toutes les étapes de la procédure de passation de marchés qui relèvent du Programme de sécurité industrielle (PSI). TPSGC fournit aussi des services reliés à la sécurité physique en regard du Programme des biens immobiliers de la TPSGC et des services communs liés à la sécurité des TI en vue d'accroître l'efficacité et les économies d'échelle du gouvernement du Canada. TPSGC est responsable de ce qui suit :

- Fournir des services qui relèvent du Programme de sécurité industrielle, y compris :
    - élaborer, en fonction d'une analyse des besoins de la collectivité et en collaboration avec le SCT, des instruments de politique, des lignes directrices et des outils dans le domaine de la sécurité des marchés aux fins d'approbation par le SCT;
    - coordonner l'élaboration et la prestation d'activités de formation et de sensibilisation liées à la sécurité des marchés;
    - diriger des groupes de travail et des comités interministériels responsables de la sécurité des marchés pour faciliter l'échange de renseignements et la collaboration entre les collectivités de pratique;
    - recueillir et examiner les pratiques exemplaires liées à la sécurité des marchés et formuler des recommandations au SCT et à des comités de gouvernance de la sécurité pour faciliter les améliorations de la politique sur la sécurité et la collaboration entre les ministères;
    - tenir à jour une base de données des organisations du secteur privé et des personnes qui ont obtenu l'autorisation d'accès à des renseignements et à des biens classifiés et protégés;
    - assumer les rôles élaborés dans les ententes internationales traitant de la sécurité industrielle;
    - procéder à des inspections de sécurité à l'égard des entreprises ayant accès à des biens et à des renseignements protégés et classifiés à l'OTAN, y compris celles inscrites aux programmes de sécurité industrielle d'alliés canadiens ou celles avec lesquels le Canada a conclu des protocoles d'entente réciproques en matière de sécurité industrielle;
    - traiter les demandes de visite lorsqu'une personne ayant une autorisation de sécurité doit visiter une organisation gouvernementale ou commerciale au Canada ou à l'étranger;
    - effectuer les enquêtes de sécurité nécessaires à l'égard des personnes et des organisations du secteur privé qui ont accès à des renseignements et à des biens protégés et classifiés, y compris celles qui participent à des marchés avec l'étranger;
    - vérifier la conformité des marchés liés à la sécurité qui donnent accès à des renseignements et à des biens du gouvernement;
    - contrôler et gérer les biens de la COMSEC pour les entreprises du secteur privé et effectuer les enquêtes de sécurité et les inspections à l'égard des biens (COMSEC) pour les entreprises du secteur privé;
    - représenter le gouvernement du Canada dans le cadre d'initiatives nationales et internationales liées à la sécurité des marchés et aux biens contrôlés;
- Fournir des services liés à la sécurité des TI, y compris :
    - fournir des services communs de sécurité des TI et d'autres solutions permettant aux ministères d'échanger de l'information avec des citoyens, des entreprises et des employés;
    - assurer la confidentialité, l'intégrité et la disponibilité des services communs de TI fournis aux ministères;
    - recueillir, analyser, regrouper et faciliter l'échange des renseignements opérationnels sur les menaces et la vulnérabilité liées aux services communs de la TI et à l'infrastructure de la TI essentiels pour le gouvernement et gérés par TPSGC, et en communiquer l'information à Sécurité publique Canada et, avec l'autorisation pertinente, aux ministères;
- Fournir des services liés à la sécurité matérielle, y compris :
    - assurer une sécurité de base dans les immeubles pour les locaux à bureaux d'utilisation générale pour lesquels TPSGC est le gardien de l'immeuble;
    - procurer des services d'agent de sécurité du Corps des commissionnaires au moyen de l'Offre à commandes principale du Corps des commissionnaires ou par d'autres fournisseurs appropriés;
- Fournir d'autres services communs, y compris :
    - attribuer des codes uniques d'identification de dossier personnel (CIDP) et, sur demande, des numéros individuels d'organisme (NIO) aux organismes extérieurs à la fonction publique fédérale;
    - tenir à jour les systèmes de CIDP et de NIO sous la direction et l'orientation du Secrétariat du Conseil du Trésor du Canada;
    - coordonner l'acquisition de biens et de services pour tous les ministères gouvernementaux lors de situations d'urgence.

Le **Service canadien du renseignement de sécurité (SCRS)** recueille, examine, analyse et conserve l'information et les renseignements dont on soupçonne qu'ils peuvent constituer une menace à la sécurité du Canada, et fournit des évaluations de sécurité aux ministères dans la mesure de son mandat prévu par la loi. Le SCRS est responsable de ce qui suit :

- élaborer, en fonction d'une analyse des besoins de la collectivité et en collaboration avec le SCT, des instruments de politique, des lignes directrices et des outils dans le domaine de la vérification de sécurité du personnel à des fins d'approbation par le SCT;
- participer à l'élaboration d'activités de formation et de sensibilisation liées à la vérification de sécurité du personnel;
- mener des enquêtes et réaliser des évaluations de sécurité à l'appui de vérifications de sécurité du personnel pour déterminer la loyauté d'une personne envers le Canada et, dans la mesure où il existe un lien avec celle-ci, sa fiabilité;
- tenir à jour un index central des évaluations de sécurité et un registre central national de l'information et de la documentation qu'il reçoit sur toutes les personnes qui sont « astreintes au secret à perpétuité » au sens de la *Loi sur la protection de l'information*;
- fournir au gouvernement des bulletins de renseignements et des évaluations sur les menaces à la sécurité du Canada, y compris sur des questions liées au terrorisme, à l'espionnage, aux activités clandestines influencées par l'étranger et à la sécurité économique, ainsi que des évaluations portant sur la cybersécurité afin de faciliter la protection des systèmes et services critiques du gouvernement du Canada;
- réaliser des analyses détaillées et intégrées de tous les renseignements disponibles sur les menaces afin de constituer une connaissance de la situation pour les décideurs du gouvernement. Dans le cadre de cette responsabilité, le SCRS est tenu :

- de réunir et d'analyser les renseignements sur des menaces potentielles provenant de tout un éventail de sources et de mettre les résultats de ces analyses à la disposition de tous les représentants du gouvernement du Canada qui le demandent (p. ex., les ASM et les praticiens de la sécurité);
- d'appuyer, grâce à ses évaluations, les postures de sécurité que doivent élaborer les premiers intervenants du gouvernement, notamment les corps de police et les organismes de gestion des urgences;
- de brosser un portrait unifié et détaillé des menaces liées à des événements spéciaux auxquels participe le gouvernement du Canada;
- d'appuyer des évaluations détaillées des menaces et des risques liés à la protection des services aux Canadiens, des opérations gouvernementales et de la confiance dans le gouvernement;
- de fournir des renseignements à SPC pour faciliter la gestion des urgences et des incidents de TI.

La **Gendarmerie royale du Canada (GRC)** assure la direction et la coordination des activités ministérielles qui aident à assurer la protection matérielle des renseignements, des biens, des installations et du personnel du gouvernement, et fournit des services liés à la prévention de la criminalité, aux enquêtes de sécurité à l'égard du personnel, aux services de police, à l'application de la loi et aux enquêtes. La GRC est responsable de ce qui suit :

- élaborer, en fonction d'une analyse des besoins de la collectivité, des instruments de politique, des lignes directrices et des outils dans le domaine de la sécurité matérielle aux fins d'approbation par le SCT;
- coordonner l'élaboration et la prestation d'activités de formation et de sensibilisation liées à la sécurité matérielle à l'intention des ASM, des praticiens de la sécurité et des autres collectivités fonctionnelles (gestionnaires de programmes, spécialistes de la gestion des locaux et du matériel, entrepreneurs);
- diriger des comités et des groupes de travail interministériels responsables de la sécurité matérielle pour faciliter le partage de l'information et la collaboration au sein de la collectivité de pratique;
- recueillir et examiner les pratiques exemplaires en matière de sécurité matérielle, et formuler des recommandations au SCT et aux comités responsables de la gouvernance de la sécurité pour faciliter les améliorations à la politique sur la sécurité et la collaboration entre les ministères;
- coordonner des recherches sur la sécurité matérielle et les enquêtes de sécurité à l'égard du personnel, et proposer des solutions au SCT et aux comités de gouvernance pour permettre au gouvernement de mieux gérer les risques et d'accroître les économies d'échelle;
- fournir aux ministères des conseils et de l'orientation sur ce qui suit :
    - la protection physique des documents, des biens et des installations du gouvernement, y compris la conception des installations,
    - l'équipement, les systèmes, les procédures et les contre-mesures de sécurité matérielle,
    - l'application des mesures de contrôle de l'accès physique, de l'élimination des supports et de la surveillance des systèmes,
    - les événements d'importance;
- fournir des services relativement à ce qui suit :
    - l'examen des moyens antitechniques de détection des intrusions et la prestation de conseils à cet égard,
    - la tenue d'enquêtes criminelles, notamment dans les domaines de l'informatique judiciaire et de la cybercriminalité,
    - la tenue d'enquêtes de sécurité à l'égard du personnel, notamment la vérification des empreintes digitales et du casier judiciaire et, s'il y a des motifs raisonnables de le faire, la réalisation d'évaluations de l'application de la loi et la communication des résultats aux ministères,
    - la protection de personnes désignées contre les menaces et les actes de violence;
- recueillir, analyser et regrouper des renseignements opérationnels sur les menaces et la vulnérabilité en ce qui concerne les vols d'identité, la sécurité matérielle, la cybercriminalité et d'autres activités criminelles pertinentes et en faciliter le partage, et communiquer cette information à SPC et au SCT ainsi que, sur la base d'une autorisation, aux ministères;
- représenter le gouvernement du Canada dans le cadre d'initiatives nationales et internationales liées à la prévention de la criminalité et la sécurité matérielle.

Bibliothèque et Archives Canada (BAC) dispense le leadership et la coordination entre les ministères gouvernementaux pour aider à assurer la conservation des informations et documents gouvernementaux. BAC est responsable de ce qui suit :

- élaborer, en fonction d'une analyse des besoins de la collectivité et du gouvernement et en collaboration avec le SCT et Sécurité publique Canada, des lignes directrices et des outils liés à la gestion des ressources informationnelles pour assurer la poursuite des activités, aux fins d'approbation par le SCT;
- conseiller les ministères du gouvernement du Canada sur la gestion des ressources informationnelles aux fins de la poursuite des activités;
- pendant une situation d'urgence, entreposer de façon sécuritaire, gérer et protéger les documents essentiels des institutions du gouvernement du Canada;
- assurer la surveillance et la présentation des rapports requis et proposer des stratégies pour acquérir les documents risquant de subir de graves dommages ou d'être détruits, qui sont essentiels pour la poursuite des activités et services du gouvernement du Canada, afin de les préserver à long terme de manière adéquate; et
- participer à la prise des mesures d'urgence pour assurer la poursuite des activités et des services du gouvernement du Canada, et donner des conseils à cet égard.

Le **ministère des Affaires étrangères et du Commerce international (MAECI)** est le principal ministère chargé d'entretenir des relations avec l'étranger et est l'autorité désignée du Canada à l'OTAN pour ce qui est de la sécurité nationale. Le MAECI est responsable de ce qui suit :

- organiser et coordonner la sécurité physique des employés du gouvernement du Canada et la sécurité matérielle des biens gouvernementaux qu'abritent les missions diplomatiques et les consulats du Canada à l'étranger;
- fournir des conseils aux ministères et procéder à des inspections périodiques et appropriées des accords en matière de

sécurité pour assurer la protection et la sécurité des renseignements classifiés de l'OTAN au Canada;
- organiser et coordonner la sécurité des visiteurs officiels dans les locaux du MAECI;
- fournir des conseils aux ministères pour faciliter la protection adéquate, aux fins de transmission et de transport, des biens se trouvant à l'étranger, et fournir des conseils sur les initiatives de sécurité menées avec des gouvernements étrangers et des organisations internationales;
- dispenser des rapports et évaluations diplomatiques au gouvernement sur les faits politiques et autres développements à l'étranger qui pourra avoir un impact sur la sécurité des biens et du personnel du gouvernement canadien;
- offrir des services de courrier diplomatique en vue du déplacement et de la protection sécuritaires des renseignements et des biens classifiés entre le Canada et les missions à l'étranger;
- assurer la confidentialité, l'intégrité et la disponibilité des communications officielles transmises par voie électronique entre les ministères et les missions diplomatiques du Canada à l'étranger;
- effectuer des enquêtes de sécurité à l'égard du personnel embauché localement et d'autres agents du gouvernement qui ne sont pas visés par le *Protocole d'entente interministériel sur les activités et le soutien des missions à l'étranger*;
- coordonner les activités dans les missions à l'étranger pendant les urgences nationales ou internationales.

Ministère de la Défense nationale (MDN) / Forces canadiennes (FC)

Le MDN / FC sont responsables de ce qui suit :

- fournir des renseignements de nature militaire à des fins d'évaluation des menaces et des risques;
- organiser et coordonner la sécurité du personnel militaire étranger en visite au Canada ou par ailleurs présent dans un établissement de défense.

École de la fonction publique du Canada (EFPC)

L'EFPC est responsable de ce qui suit :

- dispenser de la formation et offrir des services d'éducation pour que tous les fonctionnaires possèdent les connaissances et les compétences dont ils ont besoin pour procurer des résultats à la population canadienne;
- en collaboration avec le SCT et les principaux organismes responsables de la sécurité, élaborer, offrir et actualiser régulièrement les cours et les programmes qui satisfont aux besoins des collectivités fonctionnelles de gestion de la sécurité et de l'identité, déterminer si les participants y réussissent et rendre compte des résultats au SCT sur une base annuelle.