National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Revu par le CS Ex conformément à la *Loi sur l'accès à l'information* (LAI). Renseignements NON CLASSIFIÉS.

Vérification de la gestion des incidents de sécurité

Juin 2010

7050-33-2 (CS Ex)



Canada

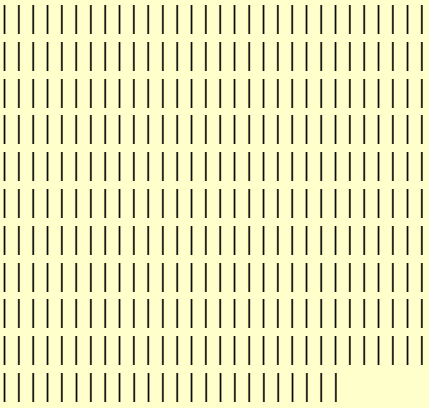
Table des matières

Liste d'abréviations

ACF	Autorité COMSEC de la formation
ASM	Agent de sécurité du Ministère
BPR	Bureau de première responsabilité
CCSS	Comité consultatif supérieur sur la sécurité
CE	Commission d'enquête
COMSEC	Sécurité des communications
CORFC	Centre d'opérations des réseaux des Forces canadiennes
CS Ex	Chef – Service d'examen
CSTC	Centre de la sécurité des télécommunications du Canada
Dir Sécur GI	Directeur – Sécurité (Gestion de l'information)
ES	Enquête sommaire
FC	Forces canadiennes
GPA Sécur	Grand Prévôt adjoint (Sécurité)
INFOSEC	Sécurité de l'information
ISSI	Incident de sécurité d'un système d'information
MDN	Ministère de la Défense nationale
ORFC	Ordonnances et règlements royaux applicables aux Forces canadiennes
OSSI	Officier de la sécurité des systèmes d'information
PGS	Politique du gouvernement sur la sécurité
PM	Police militaire
PSDN	Politique de sécurité de la Défense nationale
PSG	Politique sur la sécurité du gouvernement
RTI	Responsable du traitement des incidents
SCRS	Service canadien du renseignement de sécurité
SISEPM	Système d'information – Sécurité et police militaire
TI	Technologie de l'information
USCFC	Unité de soutien cryptographique des Forces canadiennes
VCEMD	Vice-chef d'état-major de la Défense

Sommaire des résultats

Évaluation globale



La gestion des incidents de sécurité touche l'ensemble des activités et des processus mis en place pour faire en sorte que ces incidents soient décelés et signalés, que des enquêtes soient menées et que des mesures soient prises de manière à réduire au minimum le préjudice subi et à prévenir les récidives. Ces activités et processus ont lieu par suite d'incidents de sécurité individuels ou périodiquement à un niveau stratégique, afin de protéger les biens, renseignements et services essentiels ayant trait aux opérations du ministère de la Défense nationale (MDN) et aux Forces canadiennes (FC) ainsi qu'au gouvernement du Canada.

La Politique sur la sécurité du gouvernement (PSG) (juillet 2009) stipule que lorsque des enjeux importants concernent 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, les ministères sont responsables de s'assurer :

- qu'ils font 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;
- que les mesures correctives appropriées sont prises.

La PSG exige également qu'un ASM soit nommé pour gérer le programme de sécurité ministérielle au nom des administrateurs généraux. Au moment de la vérification, le Grand Prévôt adjoint (Sécurité) (GPA Sécur) était l'ASM du MDN et des FC et donc responsable de la gestion des incidents de sécurité.

Principales constatations et recommandations

Gestion des incidents de sécurité.

Il est recommandé :

- [redacted]
- [redacted]
- [redacted]

Nota : Une liste plus détaillée des recommandations du Chef – Service d'examen (CS Ex) et des réponses de la direction figure à l'annexe A – Plan d'action de la direction.

Introduction

Contexte

La Politique du gouvernement sur la sécurité (PGS) (2002) stipulait que « les ministères doivent mettre en place des procédures de compte rendu et d'enquête relativement aux incidents de sécurité et prendre des mesures correctives pour y donner suite. Des comptes rendus et des enquêtes efficaces sur les incidents de sécurité permettent de déterminer les points faibles et de réduire le risque d'un nouvel incident de même nature »[1]. La PGS définit un incident de sécurité comme étant la « compromission d'un bien ou tout acte ou omission qui pourrait se traduire par une compromission, menaces ou actes de violence à l'encontre des employés ».[2]

La PSG, publiée en juillet 2009 pour remplacer la PGS, soulignait de nouveau la nécessité de gérer efficacement les incidents de sécurité en stipulant qu'« 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 »[3]. Elle précisait également que l'un des résultats escomptés était une gestion des incidents de sécurité « efficacement coordonnée au sein des ministères et dans l'ensemble du gouvernement »[4]. À cette fin, les ministères sont responsables de s'assurer que lorsque des enjeux importants concernent 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 :

- ils font 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;
- les mesures correctives appropriées sont prises.

La politique exige également qu'un ASM soit nommé pour gérer le programme de sécurité ministérielle au nom des administrateurs généraux. Au moment de la vérification, le GPA Sécur était l'ASM du MDN et des FC et donc responsable de la gestion des incidents de sécurité.

Gestion des incidents de sécurité

La gestion des incidents de sécurité touche l'ensemble des activités et des processus mis en place pour faire en sorte que ces incidents soient décelés et signalés, que des enquêtes soient menées et que des mesures soient prises de la façon appropriée afin de réduire au minimum le préjudice subi et de prévenir les récidives. Ces activités peuvent avoir lieu au

[1] PGS, 10.15 – Enquêtes sur les incidents de sécurité, 2002.
[2] PGS, appendice B – Glossaire, 2002.
[3] PSG, 2009, article 3.4.
[4] PSG, 2009, article 5.2.

niveau de chaque incident de sécurité, de même que du point de vue du programme ou du Ministère.

Pour chaque incident de sécurité, ces activités peuvent comprendre :

- la coordination et l'examen des évaluations des préjudices et des décisions connexes ayant trait aux mesures correctives;
- la supervision des enquêtes de sécurité et des mesures prises pour remédier aux faiblesses décelées;
- le signalement des incidents de sécurité au MDN/aux FC et à des intervenants externes au besoin.

Du point de vue du Ministère, les activités peuvent comprendre :

- la conduite d'analyses des tendances pour déterminer les récidivistes, les vulnérabilités, les changements possibles à apporter aux politiques et les possibilités de programmes de formation et de sensibilisation ciblés;
- la communication de l'information sur la sécurité à la haute direction afin d'accroître la sensibilisation à la sécurité et la prise en charge des contrôles de sécurité dans l'ensemble du Ministère.

Au moment de la vérification, les incidents de sécurité pouvaient être classés dans trois groupes techniques distincts :

1. **Incidents de sécurité des communications (COMSEC) –** Incidents de sécurité touchant le matériel COMSEC[5]. Le Directeur – Sécurité (Gestion de l'information) (Dir Sécur GI) est l'autorité COMSEC du Ministère. Un membre de la section du Dir Sécur GI 5 agit comme adjoint à l'autorité COMSEC et, à ce titre, il est le principal responsable du traitement des incidents (RTI) COMSEC.

    - D'autres intervenants clés dans la catégorie des incidents COMSEC comprennent l'Unité de soutien cryptographique des Forces canadiennes (USCFC), les autorités COMSEC des formations (ACF) et les gardiens COMSEC.

2. **Incidents de sécurité des systèmes d'information (ISSI) –** Incidents de sécurité touchant les systèmes d'information et les composantes connexes. Le Dir Sécur GI est le coordonnateur de la sécurité des technologies de l'information pour le compte du MDN et des FC, et le Dir Sécur GI 4[6] est le principal RTI dans le cas des ISSI.

[5] Comprend le matériel cryptographique, l'équipement auxiliaire, les publications COMSEC et autre matériel non cryptographique comme certains indicatifs d'appel, systèmes d'authentification et bandes-clés de formation et de maintenance.
[6] À noter que les sections du Dir Sécur GI 4 et du Dir Sécur GI 3 ont fusionné durant la vérification.

- D'autres intervenants clés dans la catégorie des ISSI comprennent le Centre d'opérations des réseaux des Forces canadiennes (CORFC), les services d'assistance des technologies de l'information (TI) et les officiers de la sécurité des systèmes d'information (OSSI).

3. **Tous les autres incidents de sécurité –** Au moment de la vérification, le GPA Sécur n'était pas seulement l'ASM, mais il était aussi responsable d'autres éléments du programme de sécurité, y compris la sécurité du matériel, du personnel et de l'information. Des membres du personnel du GPA Sécur agissent donc à titre de principaux RTI dans le cas des incidents de sécurité liés à ces domaines.

   - D'autres intervenants clés dans cette catégorie comprennent les Grands Prévôts des armées/commandements, les bureaux de sécurité locaux de la police militaire (PM) et les superviseurs de la sécurité des unités.

Outre la filière technique, la réussite du processus de gestion des incidents de sécurité dépend beaucoup de l'aptitude de tous les employés du MDN et membres des FC à reconnaître un incident de sécurité potentiel et à le signaler aux autorités compétentes. En outre, les commandants, les chefs d'établissements ou les personnes responsables doivent s'assurer que chaque incident de sécurité fait l'objet d'une enquête pour « … déterminer la nature, la cause, l'ampleur et la gravité de la situation, d'identifier les responsables de l'incident et de recommander des mesures susceptibles d'éviter que la situation ne se reproduise »[7].

Objectif

La présente vérification visait à déterminer si tous les incidents de sécurité décelés ont été signalés à l'ASM et aux organisations externes requises, si des enquêtes ont été menées et si des mesures ont été prises pour réduire au minimum le préjudice subi et/ou prévenir les récidives.

Les critères de vérification sont décrits à l'annexe B.

Portée

- La vérification a inclus une évaluation des processus utilisés par les organisations du Quartier général de la Défense nationale (principalement le GPA Sécur et le Dir Sécur GI) pour gérer les incidents de sécurité à partir du moment où ils sont signalés et jusqu'à leur conclusion.
  - Nous n'avons pas évalué les processus utilisés dans les quartiers généraux de formations, les bases/escadres ou les unités. Par conséquent, les observations formulées dans le rapport sont limitées à l'information contenue dans les dossiers d'incidents de sécurité des RTI.

[7] Politique de sécurité de la Défense nationale (PSDN), chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007, 18.10.

- Nous n'avons pas évalué la qualité ou la pertinence des enquêtes ou des évaluations des préjudices. Nous avons plutôt cherché à savoir si les RTI avaient la preuve que des enquêtes et des évaluations des préjudices avaient été effectuées et s'ils avaient fait ce type d'évaluation.

- L'échantillon de vérification a été prélevé dans les incidents de sécurité signalés au GPA Sécur, au Dir Sécur GI et au CORFC[8] et suivis par eux en 2006 et 2007. D'autres éléments de l'échantillon ont été sélectionnés parmi les incidents signalés en 2008 et au début de 2009 là où ces organisations ont indiqué que les processus avaient changé par rapport aux années précédentes.

Méthodologie

- Examen des politiques, lignes de conduite et directives du gouvernement du Canada et du MDN/des FC ayant trait aux incidents de sécurité (une liste détaillée figure à l'annexe C).
- Entrevues menées auprès de personnel des organisations du GPA Sécur, du Dir Sécur GI et du CORFC.
- Analyse des données sur les incidents de sécurité contenues dans six « systèmes » différents (c.-à-d. base de données, tableur, liste) créés par le GPA Sécur, le Dir Sécur GI et le CORFC.
- Examen d'un échantillon discrétionnaire de 69 dossiers d'incidents de sécurité.
  - L'échantillon a été prélevé, le cas échéant, à l'aide de facteurs tels que l'état, l'année, la classification, le type d'incident, le lieu, la probabilité de compromission, etc.
  - [redacted]

[8] Bien que le CORFC ne soit pas désigné comme principal RTI, les incidents de sécurité dont il a fait le suivi ont été inclus comme source distincte d'échantillonnage à cause des risques cernés durant la phase de planification relativement à la communication entre le personnel du CORFC et celui du Dir Sécur GI 4.

Constatations et recommandations

[redacted]

Signalement des incidents de sécurité à l'ASM

La principale politique du MDN et des FC sur les incidents de sécurité[9] stipule clairement que tous les incidents de sécurité doivent être signalés au GPA Sécur (anciennement le D Sécur) – l'actuel ASM. Elle reconnaît aussi qu'en négligeant de signaler un incident de sécurité ou en tardant inutilement à le faire, on s'expose à ce que des biens continuent d'être compromis ou le soient davantage.

[redacted]

- [redacted]

- [redacted]

Les facteurs qui nuisent à la capacité de s'assurer que l'ASM est informé de tous les incidents de sécurité sont les suivants :

- la façon dont les incidents de sécurité sont suivis;
- la mesure dans laquelle les processus de compte rendu sont établis, documentés, communiqués et observés.

[9] PSDN, chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007.

[redacted]

- [redacted]

- [redacted]

[redacted]

[redacted]

- [redacted]

- [redacted]

- [redacted]

[redacted]

La première étape de compte rendu permet à l'ASM de s'assurer rapidement que des mesures appropriées sont prises pour réduire au minimum le préjudice subi et empêcher que des incidents de sécurité importants ne se reproduisent et, par la suite, faciliter la conduite d'analyses des tendances ministérielles.

Évaluations des préjudices

Les politiques du MDN et des FC sur les incidents de sécurité[10] et les évaluations des préjudices[11] exigent clairement qu'une évaluation des préjudices ait lieu lors de la notification d'une compromission, réelle ou probable, de renseignements ou de biens classifiés/désignés. « L'évaluation des préjudices a pour objet de cerner les conséquences d'une compromission, réelle ou présumée, et de fournir sans délai des données sûres à l'aide desquelles on puisse recommander les mesures à prendre pour limiter le plus possible la portée des préjudices subis, par suite d'un manquement aux règles de sécurité. »[12] Les résultats d'une évaluation des préjudices, y compris un énoncé ou une analyse du préjudice causé à l'intérêt national ou à d'autres intérêts, doivent être transmis au GPA Sécur – l'autorité ministérielle chargée des évaluations des préjudices – dans les dix jours, par l'entremise du quartier général de l'unité et du commandement appropriés.

[10] PSDN, chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007.
[11] PSDN, chapitre 19 : Évaluation des préjudices, 2004.
[12] PSDN, chapitre 19 : Évaluation des préjudices, 2004, 19.07.

Selon la politique, « l'évaluation des préjudices subis doit être faite par l'auteur du document compromis, par une personne qui en avait la charge ou par quelque autre instance ayant une connaissance approfondie de la question »[13].

Une fois l'évaluation des préjudices effectuée, la politique du MDN et des FC indique que les commandants et/ou les chefs d'établissements doivent mettre en œuvre les mesures correctives connexes. Elle stipule également : « Afin que ces cas soient traités efficacement, toutes les parties concernées doivent coordonner leurs efforts et s'entendre sur les suites à donner à une affaire quand elles y ont des intérêts communs. »[14]

[13] PSDN, chapitre 19 : Évaluation des préjudices, 2004, 19.05.
[14] PSDN, chapitre 19 : Évaluation des préjudices, 2004, 19.04.

Enquêtes de sécurité

La politique du MDN et des FC sur les incidents de sécurité stipule que :

« Les manquements aux règles de sécurité doivent tous faire l'objet d'une enquête et d'un rapport, qu'ils aient entraîné ou non la compromission de renseignements classifiés ou désignés »[15]. « … les enquêtes de sécurité doivent être suffisamment approfondies pour permettre aux autorités de déterminer la nature, la cause, l'ampleur et la gravité de la situation, d'identifier les responsables de l'incident et de recommander des mesures susceptibles d'éviter que la situation ne se reproduise. »[16]

Des enquêtes de sécurité officielles sont requises en cas de compromission réelle ou possible de renseignements et/ou de biens classifiés. Il existe deux types d'enquêtes officielles : la commission d'enquête (CE) et l'enquête sommaire (ES), laquelle est moins officielle.

Selon le chapitre 18 de la PSDN, lorsque le commandant ou le chef d'établissement lui en fait la demande, le GPA Sécur est habilité à accorder une dérogation dans les cas où une enquête moins officielle est considérée comme étant aussi productive ou lorsque les circonstances ne justifient pas la tenue d'une enquête officielle.

[15] PSDN, chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007, 18.07.
[16] PSDN, chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007, 18.10.

[redacted][17].

- [redacted]
  - [redacted]
  - [redacted]

- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]

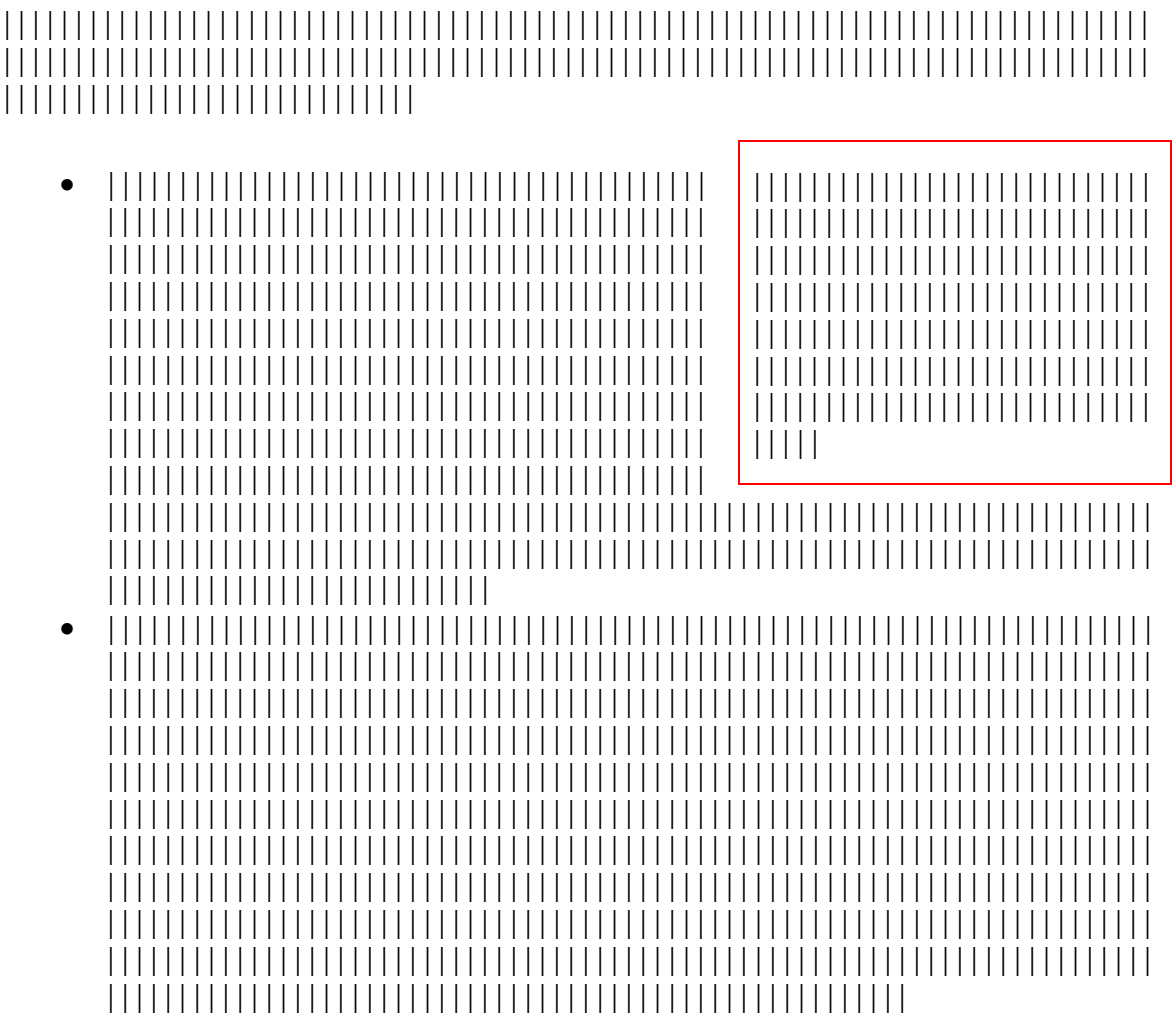
[redacted]

[17] [redacted]

- [redacted]
  - [redacted]
- [redacted]
- [redacted]
  - [redacted]

Signalement des incidents de sécurité aux organisations externes

La PGS et les normes connexes indiquent les circonstances précises dans lesquelles des incidents de sécurité doivent être signalés à des organisations à l'extérieur du Ministère. Par exemple, les incidents soupçonnés de constituer des infractions criminelles doivent être signalés aux autorités compétentes chargées de l'application de la loi, et les incidents touchant des menaces pour l'intérêt national doivent être signalés au Service canadien du renseignement de sécurité (SCRS).



- [redacted][18]

[redacted]

- [redacted]
- [redacted]
- [redacted]

Conclusion – Prévenir les récidives

[redacted]

[18] [redacted]

Recommandations

Il est recommandé :

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

BPR : ASM/VCEMD

Annexe A – Plan d'action de la direction

Gestion des incidents de sécurité

Recommandation du CS Ex

1. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

Revu par le CS Ex conformément à la *Loi sur l'accès à l'information* (LAI). Renseignements NON CLASSIFIÉS.

Annexe A

Recommandation du CS Ex

2. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Annexe A

Recommandation du CS Ex

3. [redacted]

[redacted]

[redacted]

[redacted] [redacted]

Recommandation du CS Ex

4. [redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

Annexe A

Recommandation du CS Ex

5. [redacted]

Annexe B – Critères de vérification

Objectif

1. Déterminer si les incidents de sécurité sont signalés à l'ASM et aux organisations externes requises, si des enquêtes sont menées et si des mesures sont prises pour réduire au minimum le préjudice subi et/ou prévenir les récidives.

Critères

- L'ASM est informé de tous les incidents de sécurité signalés aux RTI.
- Les préjudices sont évalués, et la direction s'engage à prendre des mesures correctives.
- Les enquêtes de sécurité sont effectuées et coordonnées de manière à obtenir toute l'information nécessaire en temps opportun, et la direction s'engage à prendre des mesures correctives.
- Les RTI entreprennent des activités (c.-à-d. des analyses des tendances) afin de réduire au minimum le risque de récidive.
- Les incidents de sécurité sont signalés aux organismes externes au besoin, conformément à la PGS et aux politiques du MDN et des FC.

Annexe C – Principales politiques sur les incidents de sécurité

Politiques de sécurité du gouvernement du Canada

Politique du gouvernement sur la sécurité, Secrétariat du Conseil du Trésor du Canada, 2002

Norme opérationnelle : Organisation et administration de la sécurité, Secrétariat du Conseil du Trésor du Canada, 1995

Norme opérationnelle de la *Loi sur la protection de l'information*, Secrétariat du Conseil du Trésor du Canada, 2003

Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information, 2004

Directives en matière de sécurité des TI : Directives pour l'application de la sécurité des communications au sein du gouvernement du Canada (ITSD-01), Centre de la sécurité des télécommunications du Canada, 2005

Conseils en matière de sécurité des TI : Manuel de contrôle du matériel COMSEC (ITSG-10), Centre de la sécurité des télécommunications du Canada, 2006

Nouvelles politiques de sécurité du gouvernement du Canada (juillet 2009)

Politique sur la sécurité du gouvernement, Secrétariat du Conseil du Trésor du Canada, 2009

Directive sur la gestion de la sécurité ministérielle, Secrétariat du Conseil du Trésor du Canada, 2009

Politiques de sécurité du MDN et des FC

Politique de sécurité de la Défense nationale, chapitre 18 : Enquêtes et rapports sur les infractions et les manquements aux règles de sécurité, 2007

Politique de sécurité de la Défense nationale, chapitre 19 : Évaluation des préjudices, 2004

Politique de sécurité de la Défense nationale, chapitre 20 : Mesures disciplinaires et administratives à l'égard des manquements aux règles de sécurité, 2004

Ordonnances et règlements royaux applicables aux Forces canadiennes, chapitre 21 : Enquêtes sommaires et commissions d'enquête, 1999

Directives et ordonnances administratives de la Défense, série 7002 : Commission d'enquête et enquêtes sommaires, 2002

Instructions relatives au contrôle du matériel SECOM (Infosec 2B), 2007

Rapports sur les incidents de sécurité des systèmes d'information (ISSI) et leur traitement au MDN, CANFORGEN 138/02 ADM IM 007/02, 2002