Centre de la sécurité des télécommunications
Communications Security Establishment

Directive en matière de sécurité des TI sur le contrôle et la gestion du matériel COMSEC en cours de réalisation

ITSD-08

Avril 2016

Canada

Avant-propos

Le document intitulé *Directive en matière de sécurité des TI sur le contrôle et la gestion du matériel COMSEC en cours de réalisation* (ITSD-08) est un document NON CLASSIFIÉ, publié avec l'autorisation du chef du Centre de la sécurité des télécommunications, conformément à la *Politique sur la sécurité du gouvernement* du Secrétariat du Conseil du Trésor du Canada.

Les demandes de renseignements généraux et les suggestions de modification doivent être transmises aux Services à la clientèle en matière de COMSEC, au Centre de la sécurité des télécommunications, par l'entremise des responsables de la COMSEC du ministère.

Le Centre de la sécurité des télécommunications informera les utilisateurs des changements apportés à la présente publication.

Date d'entrée en vigueur

La présente directive entre en vigueur au moment de sa signature.

Original signé par

le chef adjoint de la Sécurité des TI,

Scott Jones

le 25 avril 2016

Reproduction et diffusion

Table des matières

Liste des tableaux

Liste des figures

1 Introduction

1.1 Objet

La présente directive fournit aux praticiens de la sécurité des communications (COMSEC pour *Communications Security*) les exigences de sécurité minimales en matière de manutention de matériel COMSEC qu'il faut respecter lorsqu'il est impossible d'utiliser le système de comptabilité habituel compte tenu des activités d'intégration des composants ou des cartes. Dans un tel cas, il faut utiliser un système de contrôle et de comptabilité distinct appelé « système de comptabilité du matériel COMSEC en cours de réalisation » (IP pour *In-Process*). Ce matériel COMSEC sera ci-après dénommé « matériel COMSEC IP ».

Aux fins de la présente directive, les praticiens COMSEC comprennent les autorités COMSEC (parrains et planificateurs) des ministères et du secteur privé, ainsi que le personnel de garde chargé de gérer et de contrôler le matériel COMSEC IP au sein d'un compte COMSEC IP.

1.1.1 En cours de réalisation

Le terme « IP » (en cours de réalisation) est utilisé à l'échelle internationale dans les voies COMSEC pour décrire les méthodes et les registres comptables détaillés, qui permettent aux entrepreneurs de contrôler le matériel COMSEC au cours de son développement, de sa fabrication et de son assemblage.

1.2 Autorité

La présente directive est promulguée conformément à la *Politique sur la sécurité du gouvernement* (PSG) en vertu de laquelle le Centre de la sécurité des télécommunications (CST) constitue le principal organisme responsable de la sécurité et l'autorité nationale en matière de COMSEC. Le CST est responsable de l'élaboration, de l'approbation et de la promulgation des instruments de politique liés à la COMSEC et de la conception des lignes directrices et des outils s'appliquant à la sécurité des technologies de l'information (TI).

Le chef adjoint de la Sécurité des TI (CA STI) du CST est responsable de la promulgation des instruments de politique relatifs à la COMSEC.

1.3 Portée

Les méthodes de contrôle du matériel COMSEC varient selon la nature de ce matériel. La portée de la présente directive comprend :

- les clés cryptographiques ou l'équipement cryptographique (y compris les articles cryptographiques contrôlés [CCI pour *Controlled Cryptographic Items*] et les pièces, composants et ensembles COMSEC IP sensibles) qui sont en cours de développement, de fabrication, d'assemblage, de démontage, de destruction, de production ou de reproduction avant d'être contrôlés dans le Système national de contrôle du matériel COMSEC (SNCMC) ou un système COMSEC national étranger;
- l'équipement cryptographique (normalement contrôlé dans le SNCMC) qui fait l'objet d'un contrat de réparation et d'entretien et qui comprend le retrait ou l'insertion de pièces, composants ou ensembles comptables COMSEC;
- les publications COMSEC comptables (normalement contrôlées dans le SNCMC) et les manuscrits IP en cours de rédaction ou sous contrat aux fins de traduction ou de reproduction.

1.4 Contexte

La présente directive s'appuie sur la PSG et sur la *Directive sur la gestion de la sécurité ministérielle* (DGSM) et elle devrait être lue parallèlement aux publications suivantes :

- *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* (ITSD-03A);
- *Directive sur le signalement et l'évaluation des incidents COMSEC touchant le matériel COMSEC comptable* (ITSD-05);
- *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC dans le secteur privé canadien* (ITSD-06A).

1.5 Application

La présente directive s'applique aux ministères du gouvernement du Canada (GC) et aux entreprises du secteur privé autorisées à détenir du matériel COMSEC approuvé par le CST en vertu d'une entente (c.-à-d. un contrat avec le GC négocié par Services publics et Approvisionnement Canada [SPAC] ou un autre accord approuvé par le CST), ainsi qu'aux autres entités répertoriées à la section 2 qui appuient le déploiement du matériel COMSEC comptable (MCC) et d'autre matériel COMSEC IP dans les comptes COMSEC IP du GC et du secteur privé.

Aux fins de la présente directive :

- le terme « ministère du GC » comprend toutes les institutions fédérales (p. ex. ministères, agences, organismes) assujetties à la PSG et figurant aux annexes I, I.1, II, IV et V de la *Loi sur la gestion des finances publiques* (LGFP);
- le terme « autres ordres de gouvernement » inclut les organismes gouvernementaux provinciaux, municipaux et locaux (p. ex. les organismes d'application de la loi);
- le terme « entreprise du secteur privé » inclut les entreprises, organisations et personnes canadiennes qui ne figurent pas aux annexes de la LGFP ou qui ne sont pas assujetties à un gouvernement provincial ou municipal. Il désigne également les industries établies au Canada (ou autres organisations non gouvernementales) dont le Programme de sécurité industrielle (PSI) de SPAC régit la sécurité.

1.6 Résultats escomptés

L'application de la présente directive permettra d'assurer un minimum de contrôle, de protection et de comptabilité pour le matériel COMSEC approuvé par le CST et fourni à un compte COMSEC IP, ainsi que de veiller à la sécurité du matériel COMSEC en cours de développement ou de modification avant sa transition au SNCMC.

1.7 Conformité

L'attestation de la conformité aux exigences de sécurité minimales précisées dans la présente directive relève du Compte COMSEC industriel du CST (CCIC), du ministère parrain du GC et de l'entreprise concernée du secteur privé.

NOTA : À moins d'indication contraire, le terme « autorité compétente » désigne le ministère du GC responsable ou les Services à la clientèle en matière de COMSEC chargés des comptes COMSEC IP du GC, ainsi que le CCIC ou le parrain du GC pour les comptes COMSEC IP du secteur privé.

La non-conformité à la présente directive peut donner lieu à l'application de contrôles administratifs accrus à un compte COMSEC IP. Dans des circonstances extrêmes, un compte COMSEC IP sera suspendu ou fermé jusqu'à ce qu'une vérification externe soit effectuée par le CST et que les lacunes relevées pour le compte COMSEC IP soient corrigées.

1.8 Résolution de conflits

Tout conflit entre la présente directive en matière de sécurité des technologies de l'information (ITSD) et toute autre publication nationale (p. ex. une autre ITSD, la PSG ou la DGSM) ou internationale (p. ex. l'*International Traffic in Arms Regulations* [ITAR]) doit être porté à l'attention des Services à la clientèle en matière de COMSEC aux fins de résolution.

1.9 Demandes d'exception ou d'exemption

Les demandes d'exception (substitution) ou de dispense (exemption temporaire à une exigence donnée) doivent être accompagnées d'un justificatif et soumises par écrit, par l'autorité COMSEC du ministère (ACM) du GC ou du CCIC, aux Services à la clientèle en matière de COMSEC, aux fins d'approbation.

NOTA : Les Services à la clientèle en matière de COMSEC évaluent périodiquement (au moins tous les ans) la pertinence et le risque opérationnels des exceptions, de même que les progrès accomplis pour éliminer les dispenses.

1.10 Autres règlements liés à l'acquisition de matériel COMSEC

1.10.1 Propriété, contrôle et influence de l'étranger

Une entreprise du secteur privé devra normalement faire l'objet d'une évaluation de propriété, contrôle et influence de l'étranger (PCIE) dans le cadre du PSI de SPAC avant de pouvoir accéder à du MCC ou à d'autre matériel COMSEC IP en vue de s'acquitter de ses responsabilités contractuelles en matière de produits livrables ou de satisfaire à une exigence approuvée par le CST. Cette évaluation vise à s'assurer qu'il n'existe, dans les titres de propriété et les mécanismes de contrôle de l'entreprise, aucun élément susceptible de justifier un accès non autorisé au matériel COMSEC. On considèrera qu'une entreprise du secteur privé fait l'objet d'une évaluation PCIE défavorable lorsque'il y a un motif raisonnable de croire que la nature et la portée de la propriété, du contrôle et de l'influence de l'étranger sont telles que le contrôle exercé sur les activités de gestion et d'exploitation de l'installation peut mener à l'accès non autorisé au matériel COMSEC par des tiers étrangers ou leurs agents.

NOTA : Les demandes d'exemption d'une évaluation PCIE doivent être présentées aux Services à la clientèle en matière de COMSEC.

1.10.2 Programme des marchandises contrôlées du Canada

Le Programme des marchandises contrôlées (PMC) du Canada est un programme national de sécurité industrielle de SPAC qui, en vertu du *Règlement sur les marchandises contrôlées*, a le mandat de renforcer les mesures de contrôle relatives au commerce de défense du Canada et d'empêcher la prolifération de biens tactiques et stratégiques. L'acceptation des exigences de contrôle et de gestion du MCC énoncées en détail dans le présent document et dans d'autres directives du CST (y compris les ententes de contrôle du matériel COMSEC comptable [ECMCC], les protocoles d'entente, les protocoles d'accord, les ententes de non-divulgation et les accords d'assistance technique) n'exempte pas une entreprise du secteur privé de l'obligation de mettre en œuvre les exigences du PMC du Canada.

1.10.3 International Traffic in Arms Regulations des États-Unis

L'International Traffic in Arms Regulations (ITAR) est un ensemble de règlements du gouvernement des États-Unis (É.-U.) qui régissent l'exportation et l'importation des biens et services de défense énumérés dans la *United States Munitions List* (USML).

Une quantité importante de matériel COMSEC du GC provient des É.-U. L'acceptation des exigences de contrôle et de gestion du matériel COMSEC énoncées dans le présent document et dans les autres directives du CST (y compris les ECMCC, les protocoles d'entente, les protocoles d'accord et les ententes de non-divulgation) n'exempte pas un ministère du GC de mettre en œuvre les exigences de l'ITAR. Pour obtenir des conseils et des directives concernant les déplacements de matériel COMSEC assujetti à l'ITAR, prière de communiquer avec les Services à la clientèle en matière de COMSEC ou avec le CCIC, selon le cas.

1.11 Renseignements

Le tableau suivant contient les coordonnées des bureaux offrant un soutien COMSEC aux utilisateurs.

NOTA : Sauf indication contraire, les bureaux du CST reçoivent les appels téléphoniques et les transmissions par télécopieur sécurisé du lundi au vendredi, de 8 h à 16 h (heure de l'Est).

Tableau 1 – Coordonnées des bureaux COMSEC

Services à la clientèle en matière de COMSEC	
Téléphone : 613-991-8495	**Courriel :** comsecclientservices@cse-cst.gc.ca
Télécopieur sécurisé : 613-991-8565	
Compte COMSEC industriel du CST (CCIC)	
Téléphone : 613-991-7272	**Courriel :** cica-ccic@cse-cst.gc.ca
Télécopieur/télécopieur sécurisé : 613-991-7593	
Bureau national des incidents COMSEC (BNIC)	
Téléphone : 613-991-8175	**Après les heures de bureau :**
Télécopieur : 613-991-7588	**Téléphone :** 613-991-8762
Télécopieur sécurisé : Composer le 613-991-8175 pour établir la communication.	**Télécopieur sécurisé :** 613-991-8766
Courriel : ncio@cse-cst.gc.ca	**Courriel :** cansoc@cse-cst.gc.ca

1.12 Portail de l'utilisateur COMSEC

Les utilisateurs autorisés peuvent accéder au Portail de l'utilisateur COMSEC (PUC) du CST à l'adresse suivante : https://portailcomsec.cse-cst.gc.ca. Le PUC du CST fournit de l'information NON CLASSIFIÉ et PROTÉGÉ A liée à la COMSEC ainsi que des mises à niveau logicielles sur le terrain (FSU pour *Field Software Upgrade*) pour les produits, systèmes et services d'assurance élevée approuvés par le CST.
Pour devenir un utilisateur autorisé du PUC, prière de communiquer avec le Centre d'assistance en matière de matériel cryptographique (CAMC) par courriel à cmac-camc@cse-cst.gc.ca ou par téléphone au 613-991-8600.

1.13 Site Web du Centre de la sécurité des télécommunications

D'autres directives en matière de COMSEC ainsi que de l'information (au niveau NON CLASSIFIÉ seulement) ayant trait aux produits, systèmes et services d'assurance élevée approuvés par le CST sont disponibles à l'adresse suivante : https://www.cse-cst.gc.ca/fr/group-groupe/high-assurance-technologies.

1.14 Formulaires COMSEC

Les formulaires COMSEC mentionnés dans la présente directive sont disponibles dans le site Web du CST.

1.15 Transmission d'informations et de données concernant les systèmes et les services COMSEC approuvés par le CST

Les informations et les données – intégrales ou partielles – qui concernent des systèmes et des services COMSEC approuvés par le CST et pris en charge par le GC ou par un organisme parrainé par le GC peuvent être transmises électroniquement ou physiquement.

NOTA : Dans toute transmission, les extraits doivent porter la mention de classification de sécurité appropriée.

1.15.1 Transmission électronique

Les transmissions électroniques d'informations et de données concernant les systèmes et les services COMSEC approuvés par le CST doivent répondre aux directives suivantes :

- DE CONFIDENTIEL à TOP SECRET et PROTÉGÉ C – Diffusion électronique dans les réseaux du GC au moyen des capacités de chiffrement approuvées par le CST. (Ce mode de diffusion concerne la téléphonie, la télécopie et les services réseau sécurisés là où les services de communication doivent être accrédités à un niveau correspondant à celui de l'information à traiter);
- PROTÉGÉ B – Diffusion électronique dans les réseaux du GC, y compris les télécopies, ou dans des réseaux publics, pour peu que l'on garantisse une protection minimale des données et des informations par chiffrement, au moyen de l'infrastructure à clé publique (ICP) du GC;
- PROTÉGÉ A – Diffusion électronique dans les réseaux du GC ou dans les réseaux publics, pour peu que l'on garantisse une protection minimale des informations et des données par chiffrement, au moyen de l'ICP du GC, d'une connexion sécurisée au moyen du protocole HTTPS, ou d'une télécopie point-à-point non sécurisée dont l'origine et la destination se trouvent dans une zone d'opérations.

1.15.2 Transmission physique

Les transmissions physiques (par la poste ou par messagerie) d'informations et de données protégées ou classifiées concernant les systèmes et les services COMSEC approuvés par le CST doivent répondre aux directives énoncées dans l'ITSD-03A et l'ITSD-06A.

2 Rôles et responsabilités

2.1 Centre de la sécurité des télécommunications

Le CST est l'autorité nationale COMSEC. À ce titre, le CST est autorisé à remettre du matériel COMSEC au GC ou au secteur privé et est chargé d'approuver la certification, l'acquisition et l'utilisation de l'équipement et des clés cryptographiques, ainsi que d'élaborer les instruments de politique liés à la COMSEC, qui protègent les renseignements classifiés et PROTÉGÉ C.

2.1.1 Services à la clientèle en matière de COMSEC

Sous la direction du CA STI, les Services à la clientèle en matière de COMSEC sont responsables de fournir au GC et au secteur privé des conseils, de l'orientation et des directives sur la manutention des solutions et du matériel COMSEC approuvés par le CST.

Pour ce qui touche le secteur privé, les responsabilités des Services à la clientèle en matière de COMSEC incluent notamment :

- préparer une évaluation de la pertinence pour une entreprise autorisée à présenter une soumission en vue d'obtenir un contrat (p. ex. une demande de propositions) lorsque celle-ci n'a pas déjà établi de sous-compte COMSEC (consulter l'ITSD-06A);
- autoriser l'établissement ou la fermeture d'un compte COMSEC IP;
- valider les besoins du secteur privé pour ce qui est de détenir des solutions et du matériel COMSEC approuvés par le CST;
- confirmer qu'une entreprise du secteur privé ou un ministère du GC satisfait à toutes les exigences préalables et inspections de sécurité avant d'autoriser la diffusion de MCC ou d'autre matériel COMSEC à son compte COMSEC IP :
    - attestation de sécurité d'installation (ASI) ou son équivalent,
    - inspection liée à l'autorisation de détenir des renseignements (ADR) ou son équivalent,
    - inspection des mesures de protection COMSEC (IMPC),
    - inspection de la production (pour les exigences liées aux éléments IP),
    - évaluation PCIE (voir la section 1.10.1);
- coordonner la signature des ECMCC, des accords d'assistance technique, des ententes de non-divulgation et d'autres accords, le cas échéant;
- valider les plans de soutien liés au matériel de chiffrement (consulter l'ITSD-04), le cas échéant;
- coordonner la réalisation des inspections TEMPEST;
- coordonner les expéditions transfrontalières de matériel COMSEC IP avec les autres autorités responsables de la sécurité nationale.

2.1.2 Compte COMSEC industriel du CST

Sous la direction de l'ACM du CCIC, le CCIC est responsable de la gestion et du contrôle des solutions et du matériel COMSEC approuvés par le CST et attribués aux comptes COMSEC IP du secteur privé. Les responsabilités du CCIC incluent notamment :

- remplir la fonction de point de contact initial pour ce qui est de la gestion des comptes COMSEC IP (y compris le signalement des incidents COMSEC);
- veiller au respect des règles de gestion du matériel COMSEC IP, ainsi que soutenir et orienter l'utilisation de l'équipement et des clés cryptographiques approuvés par le CST;
- effectuer les vérifications des comptes COMSEC IP du secteur privé (consulter l'ITSD-06A);
- autoriser et coordonner le déplacement et la distribution du matériel COMSEC IP à l'échelle du pays (fournir des ordres de mission de messager, le cas échéant).

2.1.2.1 Autorité COMSEC du ministère du Compte COMSEC industriel du CST

Sous la direction du CA STI, l'ACM du CCIC est chargé d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme COMSEC du secteur privé qui soit conforme à la PSG et aux instruments de politique connexes en ce qui a trait à la gestion COMSEC. De plus, l'ACM du CCIC est responsable du contrôle global du matériel COMSEC approuvé par le CST qui a été imputé au CCIC.

2.2 Ministère du gouvernement du Canada

Les ministères du GC qui doivent établir un nouveau compte COMSEC du GC doivent suivre l'ITSD-03A. Toutefois, pour établir un compte COMSEC IP, les ministères du GC doivent communiquer avec les Services à la clientèle en matière de COMSEC (voir la section 3.1 de la présente directive).

2.3 Entreprise du secteur privé

Les entreprises du secteur privé qui doivent établir un nouveau sous-compte COMSEC du GC doivent suivre l'ITSD-06A. Toutefois, les entreprises du secteur privé qui veulent établir un compte COMSEC IP doivent consulter la section 3 de la présente directive.

2.3.1 Ministère parrain du gouvernement du Canada – entreprise du secteur privé

Une entreprise du secteur privé doit être parrainée par un ministère du GC, ci-après appelé « parrain du GC », qui possède un compte COMSEC en règle avant d'avoir accès au moindre MCC. L'ACM du parrain du GC doit participer activement à tous les aspects du compte COMSEC IP et les surveiller en permanence, ce qui comprend :

- informer les Services à la clientèle en matière de COMSEC qu'une entreprise du secteur privé requiert un accès au MCC;
- déterminer les besoins en matière de MCC et présenter aux Services à la clientèle en matière de COMSEC une demande d'équipement COMSEC et une demande d'autorisation pour l'achat d'équipement COMSEC dûment remplies, le cas échéant;
- fournir des inspections équivalentes aux inspections liées à l'ASI et l'ADR, ainsi qu'à l'IMPC (comme l'exige le CST) dans le cas des entreprises parrainées qui ne sont pas assujetties à un contrat du GC;
- confirmer qu'une entreprise du secteur privé répond aux exigences du PMC et de l'ITAR avant de lui confier le MCC;
- s'assurer que les Services à la clientèle en matière de COMSEC ont reçu la liste approuvée de vérification des exigences relatives à la sécurité (LVERS) du contrat, y compris les modifications, le cas échéant;
- signer l'ECMCC à titre de ministère parrain et déterminer tous les critères de prolongation;
- assigner une autorité de contrôle pour les réseaux cryptographiques autorisés, le cas échéant (consulter l'ITSD-04);
- coordonner avec le CCIC la remise du MCC à l'entreprise du secteur privé lorsque toutes les conditions préalables à l'établissement d'un compte COMSEC IP ont été satisfaites (voir la section 3), et coordonner le retrait du matériel fourni par le parrain à la fin du contrat.

2.3.2 Directeur général ou cadre supérieur clé

Le directeur général (DG) ou cadre supérieur clé, ci-après appelé « DG », de l'entreprise du secteur privé est chargé de nommer un agent de sécurité de l'entreprise (ASE). Il convient de suivre les procédures énoncées dans

le *Manuel de la sécurité industrielle* (MSI) de SPAC lorsque l'entreprise du secteur privé souhaite s'inscrire au PSI.

2.3.3 Agent de sécurité de l'entreprise

L'ASE rend compte au DG de la posture globale de la sécurité COMSEC de l'entreprise. Les responsabilités de l'ASE du secteur privé en ce qui a trait au contrôle et à la gestion du matériel COMSEC IP comprennent ce qui suit :

- coordonner la signature des ECMCC par un cadre supérieur de l'entreprise;
- veiller à la gestion du matériel COMSEC et d'autres biens IP, tel qu'il est expliqué en détail dans la présente directive et indiqué par le CCIC;
- veiller au respect des exigences de l'évaluation PCIE (voir la section 1.10.1), du PMC du Canada (voir la section 1.10.2) et de l'ITAR (voir la section 1.10.3);
- nommer le gardien COMSEC IP et le ou les gardiens COMSEC IP suppléants de l'entreprise;
- veiller à ce que le personnel de garde COMSEC IP reçoive une formation officielle du CST en matière de gestion du matériel COMSEC;
- vérifier que les exigences relatives à la gestion du matériel COMSEC sont intégrées aux consignes de sécurité de l'entreprise;
- vérifier qu'il existe une ASI de niveau approprié et que l'IMPC et les inspections liées à l'ADR et à la production ont été effectuées avant d'accepter le matériel COMSEC IP;
- veiller à ce que des séances d'initiation COMSEC soient offertes au personnel qui doit accéder au matériel COMSEC IP et à ce que celui-ci reçoive les attestations d'initiation COMSEC (des copies des attestations d'initiation COMSEC doivent être fournies au CCIC);
- analyser les exigences relatives aux visites COMSEC (c.-à-d. les visites nécessitant un accès au matériel COMSEC IP, tel qu'il est expliqué en détail dans le MSI de SPAC et dans la présente directive). Les demandes d'habilitation de sécurité des visiteurs doivent être présentées par l'entremise du PSI de SPAC. Le personnel du PSI présentera ensuite une demande d'autorisation d'accès COMSEC aux Services à la clientèle en matière de COMSEC;
- s'assurer de recevoir l'autorisation de visite du PSI avant de permettre aux visiteurs d'accéder au matériel COMSEC IP;
- élaborer un plan d'urgence COMSEC (consulter l'ITSD-06A);
- signaler les incidents COMSEC au CCIC (consulter l'ITSD-05 et l'ITSD-06A);
- veiller à ce que les sous-traitants respectent les exigences de sécurité énoncées dans le MSI de SPAC et dans la présente directive avant de leur permettre d'accéder au matériel COMSEC IP.

2.3.4 Séparation des tâches

L'ASE ne doit pas occuper le poste de gardien COMSEC IP ou de gardien COMSEC IP suppléant de l'entreprise.

2.3.5 Cumul de fonctions pour le personnel de compte COMSEC

L'ASE peut charger le gardien ou le gardien suppléant du sous-compte COMSEC de l'entreprise d'occuper simultanément le poste de gardien COMSEC IP ou de gardien COMSEC IP suppléant de l'entreprise.

2.3.6 Gardien COMSEC IP

Le gardien du compte COMSEC IP (ou gardien COMSEC IP) est responsable de la réception, de la garde, de la distribution, de la disposition ou destruction, et de la comptabilité du matériel COMSEC IP porté à son compte COMSEC IP. Ces responsabilités comprennent plus précisément :

- protéger et contrôler le matériel COMSEC IP porté au compte COMSEC IP;
- consigner la participation de l'entreprise aux contrats et aux programmes étrangers ou du GC qui requièrent un soutien en matière de MCC en ce qui a trait aux activités du compte COMSEC IP, et demeurer au fait de cette participation;
- conserver, dans les dossiers du compte, une copie de toutes les LVERS des contrats, le cas échéant, et assurer la conformité aux exigences qui concernent les activités COMSEC;
- assurer la protection et la comptabilité de tout le matériel COMSEC IP remis au compte COMSEC IP de l'entreprise ou produit dans ses installations;
- tenir à jour les registres comptables COMSEC et les documents connexes, comme il est expliqué en détail dans la présente directive;
- effectuer un inventaire du matériel COMSEC IP et présenter un rapport d'inventaire (GC-223) au CCIC, à la demande de ce dernier;
- éliminer le matériel COMSEC IP seulement lorsque les responsables le demandent et utiliser les moyens autorisés à cette fin par le CCIC;
- présenter des rapports d'inventaire, de destruction et de possession (GC-223), au besoin;
- veiller à insérer rapidement et méticuleusement toutes les modifications dans les publications COMSEC comptables (consulter l'ITSD-06A);
- s'assurer que les vérifications de pages sont effectuées pour tout le matériel COMSEC IP qui l'exige;
- connaître en permanence l'endroit où se trouve chaque article de matériel COMSEC IP détenu par l'installation ainsi que les fins auxquelles il est normalement utilisé;
- établir des procédures « internes » de contrôle strict pour chaque article de matériel COMSEC IP lorsque le matériel se trouve à l'extérieur des installations d'entreposage sécurisées du compte COMSEC IP;
- signaler immédiatement à l'ASE tous les incidents COMSEC connus ou soupçonnés;
- vérifier l'accès au matériel COMSEC IP avant d'accorder l'accès à ce matériel ou à tout document ou dossier associé au compte COMSEC IP;
- informer, par écrit, le personnel de la salle du courrier ou du service d'expédition et de réception de l'exigence de livrer directement au gardien COMSEC IP, sans les ouvrir, tous les colis ou enveloppes qui lui sont adressés ou qui portent la mention « NE PEUT ÊTRE OUVERT QUE PAR LE GARDIEN COMSEC IP ». En cas d'ouverture par inadvertance de l'emballage extérieur, l'emballage doit être livré au gardien COMSEC IP avec le colis;
- tenir une séance d'initiation COMSEC à l'intention de tout le personnel qui doit avoir accès au matériel COMSEC IP;
- veiller à ce que le matériel COMSEC IP remis dans le cadre d'un contrat spécifique ne soit pas utilisé pour un autre contrat, sauf si le parrain du GC l'autorise et, le cas échéant, en informer le CCIC;

- signaler à l'ASE ou au CCIC, selon le cas, tout problème ou toute préoccupation concernant la gestion du matériel COMSEC IP;
- s'assurer que le ou les gardiens suppléants maintiennent le niveau requis de connaissance des exigences du compte COMSEC IP afin d'assurer la gestion appropriée du compte en l'absence du gardien COMSEC IP;
- s'assurer que tout le personnel de l'entreprise qui manutentionne ou gère le matériel COMSEC IP se conforme à la présente directive;
- vérifier que les détenteurs de prêts ou les utilisateurs continuent d'avoir besoin du matériel COMSEC IP;
- informer le CCIC de tout changement concernant la gestion du compte COMSEC IP.

2.3.7 Gardien COMSEC IP suppléant

Les tâches du gardien COMSEC IP suppléant comprennent ce qui suit :

- demeurer au fait des activités courantes du compte COMSEC IP, et offrir l'aide appropriée, afin d'être en mesure d'assumer au besoin les tâches du gardien COMSEC IP sans interruption inutile des activités;
- exécuter les tâches du gardien COMSEC IP durant toute absence temporaire ne dépassant pas 60 jours civils;
- dans l'éventualité du départ permanent ou d'une absence non autorisée (61 jours civils ou plus) du gardien COMSEC IP, exécuter les tâches de ce dernier jusqu'à la nomination d'un nouveau gardien COMSEC IP.

3 Établissement ou fermeture d'un compte COMSEC IP

3.1 Établissement d'un compte COMSEC IP

Les Services à la clientèle en matière de COMSEC sont l'autorité compétente chargée d'autoriser la diffusion de matériel COMSEC au GC ou au secteur privé, ainsi que d'autoriser l'établissement des comptes COMSEC IP au sein du GC ou du secteur privé. Avant d'établir un compte COMSEC IP, un ministère du GC ou une entreprise du secteur privé qui exécute un contrat portant sur du matériel COMSEC IP doit d'abord établir un compte COMSEC du GC ou un sous-compte COMSEC d'entreprise. Les Services à la clientèle en matière de COMSEC doivent d'abord approuver un plan lié au matériel IP (voir la section 3.2) avant qu'un compte COMSEC IP ne puisse être établi. Il incombe aux Services à la clientèle en matière de COMSEC d'approuver l'établissement des comptes COMSEC IP (voir la section 2.1.1). Le compte COMSEC IP doit satisfaire aux mêmes exigences que celles qui concernent l'établissement d'un compte COMSEC ou d'un sous-compte COMSEC, selon le cas (consulter l'ITSD-03A et l'ITSD-06A). L'habilitation de sécurité associée au compte COMSEC IP doit être au moins égale au niveau de sensibilité le plus élevé du matériel COMSEC détenu au compte COMSEC IP, mais jamais inférieure au niveau SECRET.

Le compte COMSEC IP ne doit pas être inscrit dans le SNCMC, mais il relève de l'autorité responsable concernée (voir la section 1.7).

NOTA : Un gardien COMSEC du GC ou un gardien de sous-compte COMSEC d'une entreprise du secteur privé peut occuper le poste de gardien COMSEC IP lorsque les deux comptes se situent au même endroit.

3.1.1 Personnel de garde COMSEC

L'ASE doit effectuer un contrôle rigoureux des personnes sélectionnées pour jouer le rôle de gardien COMSEC IP ou de gardien COMSEC IP suppléant afin de s'assurer que chaque candidat proposé :

- est citoyen canadien (pouvant avoir une double nationalité);
- possède une habilitation de sécurité au moins égale au niveau de sensibilité le plus élevé du matériel COMSEC détenu au compte COMSEC IP, mais jamais inférieure au niveau SECRET;
- possède une attestation d'initiation COMSEC à jour;
- est une personne responsable qui est qualifiée pour assumer les fonctions et responsabilités du gardien COMSEC IP ou du gardien COMSEC IP suppléant;
- occupe un poste ou possède le niveau décisionnel qui lui donne les pouvoirs nécessaires pour exercer les responsabilités du poste;
- n'a pas auparavant été relevé de ses fonctions en tant que gardien de sous-compte COMSEC ou de gardien de sous-compte COMSEC suppléant, de gardien COMSEC IP ou de gardien COMSEC IP suppléant pour négligence ou manquement au devoir;
- n'aura pas à assumer d'autres fonctions qui nuiront à ses fonctions de gardien COMSEC IP ou de gardien COMSEC IP suppléant, et suivra une formation approuvée par le CST avant d'assumer ce rôle.

3.2 Plan lié au matériel COMSEC en cours de réalisation

Il faut préparer un plan lié au matériel COMSEC IP et le faire approuver par les Services à la clientèle en matière de COMSEC avant d'établir un compte COMSEC IP. Le plan lié au matériel COMSEC IP doit comprendre une description des données (DID pour *Data Item Description*) et une liste des données contractuelles (CDRL pour *Contract Data Requirements List*), et figurer sur la DID et la CDRL.

3.2.1 Contenu du plan lié au matériel COMSEC en cours de réalisation

Le plan lié au matériel COMSEC IP doit inclure :

- l'objet du plan lié au matériel COMSEC IP;
- les références et les définitions ayant servi à élaborer le plan lié au matériel COMSEC IP ou utilisées dans le plan;
- le nom, l'adresse et le numéro du compte COMSEC IP (si l'on connaît cette information);
- les responsabilités et tâches individuelles;
- la liste des contacts, notamment, au minimum, le nom, le numéro de téléphone et l'adresse électronique des entités suivantes :
    - bureau de gestion du projet (BGP),
    - parrain du GC de l'entreprise du secteur privé (peut également être le BGP),
    - gardien COMSEC IP ou gardien COMSEC IP suppléant,
    - ACM ou ASE, selon le cas,
    - gardien COMSEC du CCIC (pour le secteur privé),
    - Services à la clientèle en matière de COMSEC;

- les exigences en matière d'accès et d'entreposage, y compris un plan d'étage dans la mesure du possible, de même que les exigences liées aux contrôles associés aux zones jamais seul (NLZ pour *No Lone Zone*) et à l'intégrité par deux personnes (TPI pour *Two-Person Integrity*);
- la liste des articles qui doivent être contrôlés et l'étape du processus de production où l'article devient un matériel COMSEC IP et, de ce fait, est assujetti à la comptabilité IP;

  NOTA : On peut obtenir de l'aide pour déterminer ce moment, ainsi que le niveau de classification ou de protection en communiquant avec les Services à la clientèle en matière de COMSEC.
- les registres comptables (avec exemples) qui représentent l'état comptable exact de chaque article ou partie d'article IP, et ce, à chaque étape de la production, à n'importe quel moment donné;
- les processus interne et externe de rapprochement des registres comptables;
- les procédures de contrôle du matériel à toutes les étapes de sa production, de même que celles de toutes les ébauches et de tous les extraits, déchets, résidus, etc., sous quelque forme que ce soit, qui s'appliquent à cette production;
- les méthodes d'expédition pour le transfert ou la remise du matériel COMSEC IP;
- les méthodes de disposition des bris, déchets et résidus, ainsi que les autorisations et les procédures comptables qui tiennent compte de l'élimination de ces articles;
- les procédures de saisie du matériel COMSEC, du SNCMC vers le système de comptabilité IP, et la transition au SNCMC des articles réalisés;
- l'identité des sous-traitants, le cas échéant;
- les procédures de signalement des incidents COMSEC;
- un addenda au plan lié au matériel COMSEC IP pour chaque contrat dans le cadre duquel du matériel COMSEC IP est requis, qui indique quel matériel COMSEC doit être produit, modifié ou réparé en vertu du contrat et qui décrit toutes les procédures propres à ce contrat;
- toute consigne spéciale.

3.2.2 Approbation d'un plan lié au matériel COMSEC en cours de réalisation

Un plan lié au matériel COMSEC IP approuvé par les Services à la clientèle en matière de COMSEC doit avoir été mis en place avant la diffusion du matériel COMSEC IP, ou avant le début des travaux sur ce matériel, par un entrepreneur ou des sous-traitants d'un ministère du GC. Le processus d'approbation des plans liés au matériel COMSEC IP (y compris les sous-contrats) qui portent sur du matériel COMSEC assujetti à des contrôles IP est décrit dans les tableaux 2 et 3.

3.2.3 Modification d'un plan lié au matériel COMSEC en cours de réalisation

Si des modifications doivent être apportées au processus prévu de développement ou de production, le plan lié au matériel COMSEC IP doit être modifié conformément aux dispositions de la présente section. Les modifications à un plan lié au matériel COMSEC IP ne doivent pas être mises en œuvre avant l'approbation des Services à la clientèle en matière de COMSEC.

3.3 Fermeture d'un compte COMSEC IP

3.3.1 Demande de fermeture d'un compte COMSEC IP

Lorsqu'il n'est plus nécessaire de détenir du matériel COMSEC dans un compte COMSEC IP (p. ex. à la fin d'un contrat qui exige du MCC ou d'autre matériel COMSEC), l'agent de sécurité du ministère (ASM) ou l'ASE doit demander, par écrit, aux Services à la clientèle en matière de COMSEC de fermer le compte en question.

Une fois que les Services à la clientèle en matière de COMSEC ont autorisé la fermeture du compte COMSEC IP, l'ASM ou l'ASE doit :

- demander au gardien COMSEC IP de retourner tout le matériel COMSEC détenu au compte COMSEC du ministère du GC ou au CCIC (pour le secteur privé);
- fournir aux Services à la clientèle en matière de COMSEC ou au CCIC un certificat de cessation de fonction (voir le bloc D du certificat de nomination) pour chaque membre du personnel du compte COMSEC IP;
- à la réception de la confirmation de la fermeture du compte COMSEC IP des Services à la clientèle en matière de COMSEC ou du CCIC, retourner tous les dossiers du compte COMSEC IP au compte COMSEC du ministère du GC ou au CCIC.

3.3.2 Fermeture exigée par le CST

Le CST peut fermer un compte COMSEC IP dans des circonstances atténuantes. Le ministère du GC ou l'entreprise en sera alors informé par écrit.

NOTA : L'omission d'appliquer les procédures COMSEC appropriées ou d'assurer une sécurité physique adéquate, la vente ou la faillite de l'entreprise, et l'annulation d'un contrat sont des exemples de circonstances atténuantes.

3.3.3 Conditions préalables à la fermeture

On fermera un compte COMSEC IP seulement lorsque la procédure suivante aura été suivie :

- tout le matériel COMSEC a été retourné au compte COMSEC du ministère du GC ou au CCIC, de sorte que le solde du compte COMSEC IP est maintenant nul;
- l'ASM ou l'ASE a transmis les certificats de cessation de fonction (voir le bloc D du certificat de nomination) ainsi que tous les dossiers du compte COMSEC IP.

3.3.4 Confirmation de la fermeture

Lorsque le CCIC a confirmé que les conditions préalables à la fermeture ont été satisfaites, l'ASM ou l'ASE est informé par écrit que le compte COMSEC IP a été fermé et que le personnel de garde du compte COMSEC IP a été relevé de ses responsabilités à l'égard du compte.

Jusqu'à ce qu'ils aient reçu un avis formel du CCIC ou des Services à la clientèle en matière de COMSEC, le gardien COMSEC IP et le gardien COMSEC IP suppléant demeurent responsables du compte COMSEC IP et de tout écart concernant le matériel COMSEC connexe.

Tableau 2 – Processus d'approbation d'un plan lié au matériel COMSEC IP

Étape	Mesure
1	Le ministère du GC ou l'entreprise du secteur privé (en collaboration avec le parrain du GC) doit fournir une ébauche du plan lié au matériel COMSEC IP aux Services à la clientèle en matière de COMSEC 90 jours civils avant le début des travaux IP, ou plus tôt dans la mesure du possible.
2	Les Services à la clientèle en matière de COMSEC examinent l'ébauche du plan lié au matériel COMSEC IP et donnent leurs commentaires au ministère du GC ou à l'entreprise du secteur privé, le cas échéant.
3	Une fois que le CST détermine que le plan est acceptable (et si l'entente contractuelle l'exige), le ministère du GC ou l'entreprise du secteur privé doit officiellement soumettre le plan lié au matériel COMSEC IP au bureau de coordination des contrats ou au BGP du ministère client du GC, et en transmettre une copie à l'autorité compétente (voir la section 1.7).
4	Le CST fournit une approbation officielle au ministère du GC et à l'entreprise du secteur privé. L'autorité compétente doit signer l'approbation du plan lié au matériel COMSEC IP (voir l'étape 3).

Tableau 3 – Processus d'approbation d'un plan lié au matériel COMSEC IP d'un sous-traitant

Étape	Mesure
1	L'entrepreneur principal doit veiller à ce que les exigences qui s'appliquent au plan lié au matériel COMSEC IP (telles qu'elles sont indiquées dans la présente section) soient précisées dans le contrat avec le sous-traitant.
2	L'entrepreneur principal doit s'assurer que le sous-traitant élabore un plan lié au matériel COMSEC IP.
3	L'entrepreneur principal examine l'ébauche du plan lié au matériel COMSEC IP et fournit des commentaires au sous-traitant, le cas échéant.
4	En collaboration avec le parrain du GC, l'entrepreneur principal doit soumettre une ébauche du plan lié au matériel COMSEC IP aux Services à la clientèle en matière de COMSEC au nom du sous-traitant 90 jours civils avant le début des travaux IP, ou plus tôt dans la mesure du possible.
5	Le CST examine l'ébauche du plan lié au matériel COMSEC IP et fournit des commentaires à l'entrepreneur principal, le cas échéant.
6	Une fois que le CST détermine que le plan est acceptable et si l'entente contractuelle l'exige, l'entrepreneur principal doit officiellement soumettre le plan lié au matériel COMSEC IP au bureau de coordination des contrats ou au BGP du ministère du GC et en transmettre une copie au CCIC et au sous-traitant.
7	Le CST fournit une approbation officielle au ministère du GC et à l'entrepreneur principal.

4 Comptabilité du matériel COMSEC en cours de réalisation

4.1 Système comptable du matériel COMSEC en cours de réalisation

Le gardien COMSEC IP doit utiliser un système comptable IP approuvé par le CST pour la comptabilité du matériel COMSEC IP.

4.2 Comptabilité du matériel COMSEC en cours de réalisation

Les registres comptables IP doivent contenir les renseignements suivants pour chaque article :

- la date à laquelle l'article a été inscrit dans le système comptable IP au sein de l'installation (y compris les articles IP retournés par un sous-traitant ou le gouvernement, ou retournés pour être remaniés);
- une brève description non classifiée des articles à contrôler, qui peut comprendre l'un ou plusieurs des éléments suivants :
  - le numéro de nomenclature de l'Organisation du traité de l'Atlantique nord (OTAN),
  - le numéro de nomenclature fédéral des É.-U.,
  - numéro de pièce du fournisseur ou du CST,
  - le titre abrégé (le cas échéant),
  - la sensibilité (niveau de classification ou de protection, ou CCI – voir la section 6.2),
  - le code de comptabilité (CC), le cas échéant,
  - la quantité (lorsque la comptabilité par quantité est approuvée) ou le numéro de série (s'il faut comptabiliser chaque article);
- la disposition :
  - l'intégration à un ensemble supérieur (préciser l'ensemble supérieur) ou l'intégration à un autre article de matériel COMSEC IP,
  - le transfert ou la remise conformément aux procédures de comptabilité IP,
  - l'inscription dans le SNCMC en tant qu'article comptable individuel,
  - la destruction ou la déclassification,
  - la réinscription comme matériel IP pour remaniement,
  - toute autre mesure non prévue aux paragraphes ci-dessus.

4.3 Rapprochement des registres comptables liés au matériel COMSEC en cours de réalisation

Le gardien COMSEC IP et un témoin détenant l'habilitation de sécurité appropriée et ayant assisté à une séance d'initiation COMSEC doivent effectuer le rapprochement des registres comptables IP deux fois par année et à la livraison finale du matériel COMSEC. Au moyen d'un contrôle à vue du matériel COMSEC, le rapprochement doit déterminer que chaque article porté au système de comptabilité IP ou produit dans le cadre d'un processus IP est comptabilisé afin d'assurer que celui-ci :

- fait toujours partie du processus IP ou qu'il a été intégré ou détruit;
- est entreposé comme matériel COMSEC IP;
- a été transféré dans le cadre de la livraison d'un matériel COMSEC terminé;
- a été transféré ou remis à un entrepreneur, à un sous-traitant ou au ministère client du GC.

Tout article dont on ne peut rendre compte doit être signalé sur-le-champ comme **incident COMSEC**, tel qu'il est expliqué en détail dans l'ITSD-05.

NOTA : Les Services à la clientèle en matière de COMSEC ou le CCIC peuvent demander que le rapprochement des registres soit effectué à des intervalles irréguliers.

5 Rapports comptables liés au matériel COMSEC en cours de réalisation

5.1 Généralités

Les sections suivantes décrivent les rapports qui font le suivi du matériel COMSEC IP dans différentes circonstances.

5.2 Déplacement de matériel COMSEC en cours de réalisation

Le gardien COMSEC IP doit transférer le matériel COMSEC IP du compte COMSEC IP à un autre compte COMSEC IP au moyen d'un rapport de transfert (GC-223) sur lequel doit figurer le numéro de transaction du matériel COMSEC IP. Le rapport de transfert doit stipuler que le matériel COMSEC est du matériel COMSEC IP et indiquer le motif du transfert, par exemple, « fourni à l'appui du contrat (insérer le numéro) ». Il faut annoter les registres comptables IP pour rendre compte du transfert en y inscrivant le numéro de transaction du matériel COMSEC IP qui figure sur le rapport de transfert.

5.3 Réception du rapport de transfert du matériel COMSEC en cours de réalisation

Un gardien COMSEC qui reçoit du matériel COMSEC IP d'un autre compte doit signer les deux copies du rapport de transfert qui accompagne le matériel COMSEC IP afin d'attester la réception et l'intégrité du matériel COMSEC IP. Il doit aussi y attribuer un numéro de transaction IP entrant à des fins de suivi, en garder une copie et envoyer l'autre au gardien COMSEC qui a expédié le matériel pour ses dossiers. Il doit ensuite annoter les registres comptables IP pour rendre compte de la réception du matériel.

5.4 Accusé de réception du matériel COMSEC en cours de réalisation

Lorsqu'il remet du matériel COMSEC IP à un détenteur de prêt avant l'acceptation du produit final par le GC, le gardien COMSEC IP doit le faire moyennant un accusé de réception (GC-223). Il doit attribuer un numéro de transaction IP sortant à l'accusé de réception et fournir les renseignements indiqués à la figure 1. Le prêt ne devrait pas excéder une période de 90 jours civils sans être renouvelé. Il faut mettre à jour les registres comptables IP pour rendre compte de la remise du matériel. Le matériel COMSEC IP doit être expédié directement au détenteur de prêt. Le détenteur de prêt doit signer et retourner une des copies.

5.5 Transfert suivant l'acceptation par le gouvernement du Canada

Après l'acceptation et l'achat par le GC, le gardien COMSEC IP doit transférer le matériel COMSEC IP du compte COMSEC IP au compte COMSEC du parrain du GC ou au sous-compte COMSEC de l'entreprise afin que le matériel COMSEC IP soit inscrit dans le SNCMC. Le rapport de transfert doit porter dans la colonne « remarques » la mention « NOUVEAU MATÉRIEL COMSEC ».

Dans le cas du matériel qui sera inscrit dans le sous-compte COMSEC de l'entreprise, le gardien du sous-compte COMSEC doit remplir un rapport de possession (GC-223) pour inscrire le matériel COMSEC dans le SNCMC. Le matériel doit ensuite être acheminé à l'autorité compétente (voir la section 1.7), qui coordonnera ensuite le transfert du matériel COMSEC au parrain du GC.

5.6 Diffusion temporaire au gouvernement du Canada

S'il faut diffuser temporairement du matériel COMSEC IP au GC, une copie de l'accusé de réception (GC-223) doit être fournie au compte COMSEC auquel le détenteur de prêt qui reçoit le matériel est inscrit (ou à l'ASM si le ministère du GC n'a pas de compte COMSEC). Le matériel COMSEC IP ne doit pas être inscrit dans le SNCMC.

NOTA : Le gardien COMSEC IP doit communiquer avec le gardien COMSEC ou l'ASM pour confirmer que le détenteur de prêt détient l'habilitation de sécurité appropriée, qu'il a reçu une initiation COMSEC et qu'il peut entreposer le matériel COMSEC IP de manière sécurisée.

5.7 Renouvellement d'accusés de réception

Le gardien COMSEC IP doit examiner les accusés de réception au moins tous les 90 jours civils afin de s'assurer que le matériel COMSEC IP est retourné avant la date d'échéance. Si l'accusé de réception doit être renouvelé, le gardien COMSEC IP doit préparer un nouvel accusé de réception comportant un nouveau numéro de transaction IP et portant en référence le numéro de transaction de l'accusé de réception précédent. L'accusé de réception doit comprendre les renseignements supplémentaires donnés à la figure 1. Le détenteur de prêt doit signer le nouvel accusé de réception à chaque renouvellement.

5.8 Retour du matériel COMSEC en cours de réalisation

Lorsque le matériel COMSEC IP doit être retourné au compte COMSEC IP, le gardien COMSEC IP doit préparer un accusé de réception pour le détenteur de prêt. Le détenteur de prêt doit inclure cet accusé de réception dans le colis. Dès la réception du matériel, le gardien COMSEC IP signera l'accusé de réception et en enverra une copie au détenteur de prêt. L'accusé de réception doit comporter les renseignements supplémentaires fournis à la figure 2.

5.9 Rapport de destruction de matériel COMSEC en cours de réalisation

Le gardien COMSEC IP doit préparer un rapport de destruction (GC-223) afin de rendre compte de la destruction d'un matériel COMSEC dans le système de comptabilité IP. Le rapport de destruction doit être signé par le gardien COMSEC IP et le témoin ayant effectué la destruction. Il faut inscrire dans la colonne « remarques » du rapport de destruction le motif de la destruction (p. ex. bris, déchets, résidus).

NOTA : Le personnel qui procède à la destruction doit posséder une habilitation de sécurité au moins égale au niveau de sensibilité le plus élevé du matériel COMSEC détruit, mais jamais inférieure au niveau SECRET.

Le matériel COMSEC IP énuméré ci-dessus n'a pas été accepté par le gouvernement du Canada et est la propriété de :

_____.
(Nom)

Le présent matériel COMSEC IP est remis (en vertu d'un accusé de réception) pendant 90 jours civils pour :

_____.
(Raison du prêt)

Si la durée du prêt dépasse 90 jours civils, le destinataire doit signer un nouvel accusé de réception fourni par :

_____.
(Nom)

CE MATÉRIEL COMSEC IP NE DOIT PAS ÊTRE INSCRIT
DANS LE SYSTÈME NATIONAL DE CONTRÔLE DU MATÉRIEL COMSEC (SNCMC).

Figure 1 – Renseignements à fournir sur un accusé de réception de matériel COMSEC IP

Le matériel COMSEC IP énuméré ci-dessus n'a pas été accepté par le gouvernement du Canada et est la propriété de :

_____.
(Nom de l'entrepreneur)

Ce matériel COMSEC IP est retourné à l'auteur.

CE MATÉRIEL COMSEC IP **NE** DOIT **PAS** ÊTRE INSCRIT
DANS LE SYSTÈME NATIONAL DE CONTRÔLE DU MATÉRIEL COMSEC (SNCMC).

Figure 2 – Retour d'un matériel COMSEC en cours de réalisation remis

6 Contrôle de l’équipement cryptographique en cours de réalisation

6.1 Circuits intégrés

6.1.1 Articles individuels

Chaque article IP classifié ou protégé (p. ex. tranche, masque, réticule, dessin maître, échantillon d’essai, bande de génération de combinaisons logiques, etc.) doit être contrôlé au moyen d’un système continu d’accusés de réception, d’un processus de fabrication à un autre et d’un compte COMSEC IP à un autre. Le registre de comptabilité et de contrôle doit indiquer la réception ou la fabrication de chaque article IP, la description et la quantité de matériel COMSEC et la disposition de l’article; on doit également y retrouver la signature de chaque personne responsable (p. ex. surveillant de la production, détenteur de prêt) pour chaque étape de la fabrication.

6.1.2 Articles partiels

Les parties d’une tranche incomplète doivent être contrôlées en tant que puces individuelles, conformément à la section 6.1, à moins que la tranche ne soit reconstruite sur une base adhésive. Dans un tel cas, le nombre de tranches doit à nouveau servir de base de comptabilité et le nombre de puces enlevées doit figurer au registre. On devrait essayer de déterminer le nombre de puces susceptibles d’être complètes dans une tranche avant de découper cette dernière en puces élémentaires.

Si on ne peut pas le faire, alors le nombre de puces complètes doit être établi immédiatement après le découpage de la tranche. Une puce incomplète doit être considérée comme un résidu classifié ou protégé, et doit être contrôlée en conséquence.

6.1.3 Articles brisés

Toute aire dans laquelle une tranche, un masque, un réticule ou une puce IP a été brisé doit être protégée sur-le-champ. Tous les efforts doivent être déployés pour tenter de reconstruire l’article brisé sur une base adhésive. S’il manque une puce, en totalité ou en partie, il faut remplir un rapport d’incident COMSEC initial, conformément aux dispositions de l’ITSD-05. S’il manque un morceau ou si l’ensemble de la tranche, du masque, du réticule ou de la puce a été fragmenté au point où il est impossible de reconstruire l’original, le gardien COMSEC IP doit procéder comme suit :

1. enlever toutes les particules de l’aire où le bris s’est produit au moyen d’un aspirateur;
2. inscrire sur le sac contenant les résidus de l’article le numéro de la tranche, du masque ou du réticule (ou, le cas échéant, l’identification de la puce ou de la partie de celle-ci appartenant au numéro de la tranche, du masque ou du réticule) et sa sensibilité;
3. veiller à ce que deux personnes ayant l’habilitation appropriée apposent leurs initiales sur le sac de l’aspirateur;
4. contrôler le sac de l’aspirateur comme étant du matériel COMSEC protégé ou classifié, le cas échéant, jusqu’à ce que son contenu puisse être détruit au moyen d’une méthode de destruction approuvée par le CST ou être transporté au CCIC (dans le cas des comptes COMSEC IP du secteur privé).

6.2 Articles cryptographiques contrôlés

6.2.1 Développement

Le développement, la fabrication ou le montage d'un équipement CCI IP peut être entrepris :

- soit à partir d'une conception IP qui évolue durant le développement jusqu'à devenir un ensemble ou un composant CCI IP que l'entrepreneur transforme ensuite en équipement CCI IP;
- soit à partir d'un composant ou d'un ensemble CCI que l'entrepreneur reçoit d'une source autorisée, puis transforme en un équipement CCI IP.

6.2.2 Protection des fonctions de matériel COMSEC en cours de réalisation

Les puces à microcircuit utilisées dans les applications matérielles ou micrologicielles doivent être protégées par un revêtement approuvé par le CST et capable de résister aux tentatives :

- de récupérer les renseignements descriptifs IP par rétroingénierie;
- de mettre en échec les dispositifs de sécurité;
- de récupérer autrement l'information en mémoire (p. ex. au moyen d'une sonde externe), sauf si, après vérification du parrain du GC par l'entremise des Services à la clientèle en matière de COMSEC :
    - le revêtement protecteur est incompatible avec la puce à microcircuit de telle sorte que la réduction d'efficacité entraînée par l'utilisation de ce revêtement est inacceptable,
    - ou d'autres mesures de protection tout aussi valables ont été adoptées pour faire face aux menaces susmentionnées.

NOTA 1 : À moins que le procédé soit impossible du point de vue technique, les applications matérielles de fonctions COMSEC IP doivent être sous forme de microcircuits personnalisés (autrement dit, il est interdit d'incorporer des composants discrets ou des microcircuits standards).

NOTA 2 : Les applications micrologicielles de fonctions COMSEC IP doivent être sous forme de microcircuits (personnalisés ou standards). Ceux-ci doivent être dotés d'un dispositif irréversible de sécurité qui empêche d'extraire ou de modifier l'information programmée dans la mémoire interne à partir de broches physiques accessibles de l'extérieur.

6.2.3 Transition de l'état de conception de matériel COMSEC en cours de réalisation à l'état d'article cryptographique contrôlé en cours de réalisation – applications matérielles

Dans le cas des applications matérielles, la transition de l'état de conception de matériel COMSEC IP à celui de CCI IP s'effectue à l'étape de la réalisation du photomasque de microcircuits. Les sous-produits de la conception automatisée menant au réticule de chaque couche du circuit intégré, et incluant ce réticule, doivent être manutentionnés au même niveau de classification ou de protection que les dessins techniques desquels ils découlent. Les photomasques utilisés au bout du compte comme outillages dans le processus réel de production, tout comme les tranches à semi-conducteurs qui en résultent et leurs formes subséquentes (p. ex. des puces individuelles) et qui aboutissent à des dispositifs scellés, doivent être contrôlés en tant que CCI IP, conformément à la section 6.2.5.

6.2.4 Transition de l'état de conception de matériel COMSEC en cours de réalisation à l'état d'article cryptographique contrôlé en cours de réalisation – applications micrologicielles

Dans le cas des applications micrologicielles, la transition de l'état de conception de matériel COMSEC IP à celui de CCI IP s'effectue une fois que les renseignements descriptifs IP ont été entrés dans la mémoire du microcircuit et que la fonction de sécurité décrite à la section 6.2.2 a été réglée. Par la suite, les microcircuits doivent être contrôlés en tant que CCI IP, conformément aux dispositions de la section 6.2.6. Les données de base des logiciels utilisés pour les applications micrologicielles des renseignements descriptifs IP continuent de porter la mention IP et doivent être protégées conformément aux dispositions de la présente directive.

6.2.5 Contrôle des dispositifs à microcircuit en cours de réalisation

Après leur transition de l'état de conception du matériel COMSEC IP à celui de CCI IP, les dispositifs à microcircuit doivent être contrôlés durant tout le reste du processus de fabrication et d'assemblage de la façon suivante :

- **les photomasques et les tranches doivent :**
  - être clairement marqués « ARTICLE CRYPTOGRAPHIQUE CONTRÔLÉ » ou « CCI »,
  - porter un numéro de série et être comptabilisés à l'aide de ce numéro (jusqu'à ce que les photomasques soient détruits en toute sécurité et que les tranches soient découpées en puces),
  - être comptabilisés par quantité une fois qu'une tranche a été découpée en puces;
- lorsqu'un microcircuit est complètement fabriqué, acheté, accepté et ensuite transféré au gouvernement, la comptabilité doit se faire conformément aux procédures comptables du SNCMC;
- lorsqu'un microcircuit est complètement fabriqué, acheté, accepté et ensuite expédié à une autre entreprise du secteur privé pour être utilisé dans un processus de fabrication, la comptabilité doit se faire conformément aux procédures de comptabilité IP;
- lorsqu'un microcircuit est entreposé en vue d'une vente future ou en raison d'obligations contractuelles, ou lorsqu'il passe au niveau de montage suivant, sa comptabilité doit se poursuivre dans le système de comptabilité IP de l'entrepreneur.

6.2.6 Contrôle des cartes imprimées logiques

Une carte imprimée logique (PWA pour *Printed Wiring Assembly*) passe à l'état CCI IP dès qu'un microcircuit CCI y est posé. Dès lors, la PWA doit être contrôlée comme suit durant le reste du processus de fabrication et de montage :

- au moment de la transition, la comptabilité du microcircuit prend fin et celle de la PWA commence;

  NOTA : La disposition du microcircuit et la comptabilité de la PWA qui s'ensuit doivent être indiquées dans les registres comptables IP.
- les PWA entièrement fabriquées sont comptabilisées en fonction de la quantité lorsqu'elles correspondent à la définition de « composant CCI », et par numéro de série lorsqu'elles correspondent à la définition d'« ensemble CCI »;
- à toute étape ultérieure du montage, les PWA doivent être comptabilisées en fonction de la quantité;
- lorsqu'une PWA est entièrement fabriquée, achetée, acceptée et ensuite transférée au gouvernement, la comptabilité doit se faire conformément aux procédures comptables du SNCMC;

- lorsqu'une PWA est entièrement fabriquée, achetée et ensuite expédiée à une autre entreprise du secteur privé pour être utilisée dans un processus de fabrication, la comptabilité doit se faire conformément aux procédures de comptabilité IP;
- lorsqu'une PWA est entreposée en vue d'une vente future ou en raison d'obligations contractuelles, ou lorsqu'elle passe à une étape suivante du montage, sa comptabilité doit se poursuivre dans le système de comptabilité IP de l'entrepreneur.

6.2.7 Étiquetage des composants, des ensembles et de l'équipement marqués « Article cryptographique contrôlé »

Les composants, les ensembles et l'équipement CCI doivent porter la mention « ARTICLE CRYPTOGRAPHIQUE CONTRÔLÉ » ou « CCI » selon l'espace disponible pour apposer l'étiquette, conformément aux dessins standards disponibles auprès des Services à la clientèle en matière de COMSEC et aux renseignements fournis au tableau 4.

Tableau 4 – Étiquetage CCI

CCI	Exigences en matière d'étiquetage et de contrôle
Composants	• Chaque composant CCI (dispositif à microcircuit CCI) doit être étiqueté « CCI » au même moment où est appliquée une autre nomenclature propre aux pièces.
Ensembles	• Chaque ensemble CCI (carte équipée logique) doit porter un numéro de série du gouvernement aux fins de comptabilité, conformément aux critères que fourniront les Services à la clientèle en matière de COMSEC. • L'étiquetage peut se faire à n'importe quelle étape du processus de montage avant la fin de ce dernier. • Un ensemble CCI passe à l'état CCI dès qu'on y installe un composant CCI (microcircuit CCI) (voir la section 6.2.6).
Équipement	• Chaque article d'équipement CCI doit être étiqueté « ARTICLE CRYPTOGRAPHIQUE CONTRÔLÉ » à un endroit bien en vue sur l'extérieur. • Chaque article d'équipement CCI doit également porter un numéro de série du gouvernement aux fins de comptabilité, conformément aux critères fournis par les Services à la clientèle en matière de COMSEC. • L'étiquetage peut se faire à n'importe quelle étape du processus de montage avant la fin de ce dernier. • Un équipement passe à l'état CCI dès qu'on y installe un composant CCI (microcircuit CCI) ou un ensemble CCI (carte équipée logique).

6.3 Bris, déchets et résidus de matériel COMSEC en cours de réalisation

Si du matériel COMSEC IP est rejeté du processus de développement, de production, de fabrication ou de montage en raison d'une défectuosité, d'un bris ou d'une perte normale (p. ex. tranche brisée, puce partielle, dispositif à microcircuit ou PWA brisés ou défectueux), il doit être contrôlé jusqu'à ce que sa destruction approuvée soit effectuée. Lorsque les méthodes de destruction autorisées ne sont pas disponibles, il faut communiquer avec les Services à la clientèle en matière de COMSEC ou le CCIC pour obtenir des conseils relativement à l'élimination.

6.4 Perte de matériel COMSEC en cours de réalisation

Tout matériel COMSEC IP perdu doit faire l'objet d'une recherche exhaustive. La perte d'un tel matériel doit être documentée dans les registres comptables COMSEC IP et communiquée sur-le-champ en tant qu'**incident COMSEC**, tel qu'il est expliqué en détail dans l'ITSD-05.

7 Équipement cryptographique assujetti à un contrat de réparation et d'entretien

7.1 Transfert à destination ou en provenance de l'entrepreneur

Le gardien COMSEC du ministère du GC doit transférer l'équipement cryptographique nécessitant des réparations ou de l'entretien au sous-compte COMSEC de l'entrepreneur par l'intermédiaire du CCIC, sauf si ce dernier a préapprouvé un transfert direct. Le gardien du sous-compte COMSEC transférera l'équipement cryptographique au compte COMSEC IP et annotera l'accusé de réception (GC-223) de manière appropriée. Le processus sera inversé lorsque l'équipement sera prêt à être retourné au ministère du GC.

7.2 Comptabilité du matériel COMSEC en cours de réalisation au sein de l'installation de réparation et d'entretien

Il faut veiller à ce que les procédures de comptabilité du matériel IP consignent le retrait, l'insertion, la disposition, la destruction (si elle a été autorisée) et la conversion (au besoin) de toutes les pièces COMSEC et de tous les composants et ensembles COMSEC utilisés dans le processus de réparation et d'entretien, de même que la comptabilité continue de l'équipement cryptographique faisant l'objet de réparations ou d'entretien à l'installation de l'entrepreneur ou au dépôt de maintenance.

7.3 Sources des pièces, composants et ensembles COMSEC de rechange

7.3.1 Sources internes

Si l'entrepreneur chargé de la réparation et de l'entretien a aussi construit l'équipement cryptographique, les pièces, composants et ensembles COMSEC nécessiteront un rapport de transfert interne (GC-223) depuis le système de comptabilité IP du processus de fabrication au système de comptabilité IP du processus de réparation et d'entretien.

7.3.2 Sources gouvernementales

Le gardien COMSEC doit transférer les pièces, composants et ensembles COMSEC au CCIC qui, à son tour, remettra le matériel en tant qu'équipement fourni par le gouvernement à un sous-compte COMSEC du secteur privé.

7.3.3 Sous-traitance

Les pièces, composants et ensembles COMSEC qui proviennent d'un autre entrepreneur du secteur privé, en vertu d'une entente contractuelle ou à la suite d'un achat, devraient être transférés du système de comptabilité IP du fabricant au système de comptabilité IP de l'entrepreneur chargé de la réparation et de l'entretien au moyen d'un rapport de transfert du matériel IP.

7.4 Pièces, composants ou ensembles COMSEC en cours de réalisation non utilisables

Toute pièce ou tout composant ou ensemble COMSEC retiré d'un équipement cryptographique du GC et remplacé par du matériel COMSEC IP (pièce, composant ou ensemble) devient automatiquement du matériel COMSEC IP non utilisable destiné à la disposition. À moins d'obtenir une autorisation des Services à la clientèle en matière de COMSEC, ces articles non utilisables doivent être transférés au CST par les voies COMSEC aux fins de disposition. Les registres de disposition du matériel IP doivent indiquer la disposition et, au besoin, le remplacement des pièces, composants et ensembles COMSEC non utilisables. La disposition du matériel COMSEC IP doit être détaillée dans le plan lié au matériel COMSEC IP.

7.5 Équipement cryptographique non réparable

L'équipement cryptographique, assujetti à un contrat de réparation et d'entretien, qu'il est impossible de réparer doit être retourné au ministère du GC par l'entremise du CCIC aux fins d'élimination. L'entrepreneur chargé de la réparation et de l'entretien n'est autorisé à disposer d'un équipement cryptographique d'un ministère du GC qu'en le retournant à ce ministère. Le ministère du GC est responsable de la disposition de son équipement cryptographique conformément à l'ITSD-03A.

8 Élaboration de publications COMSEC comptables

Il est possible que les ministères du GC doivent élaborer des publications COMSEC qui devront être comptabilisées, contrôlées et gérées à partir du SNCMC. Les ministères du GC qui se préparent à élaborer des publications COMSEC comptables doivent communiquer avec les Services à la clientèle en matière de COMSEC afin d'obtenir une approbation et des conseils.

9 Reproduction ou traduction de publications COMSEC comptables

Il est possible que les ministères du GC doivent reproduire ou traduire des publications COMSEC qui sont comptabilisées, contrôlées et gérées à partir du SNCMC. Les ministères du GC qui reproduisent ou traduisent des publications COMSEC comptables doivent communiquer avec les Services à la clientèle en matière de COMSEC afin d'obtenir une approbation et des conseils.

10 Références

10.1 Abréviations et sigles

ACM	Autorité COMSEC du ministère
ADR	Autorisation de détenir des renseignements
ASE	Agent de sécurité de l'entreprise
ASI	Attestation de sécurité d'installation
ASM	Agent de sécurité du ministère
BGP	Bureau de gestion de projets
BNIC	Bureau national des incidents COMSEC
CA STI	Chef adjoint, Sécurité des technologies de l'information
CAMC	Centre d'assistance en matière de matériel cryptographique
CC	Code de comptabilité
CCI	Article cryptographique contrôlé (*Controlled Cryptographic Item*)
CCIC	Compte COMSEC industriel du CST

CDRL	Liste des données essentielles au contrat (*Contract Data Requirements List*)
COMSEC	Sécurité des communications (*Communications Security*)
COR	Bureau central des dossiers (*Central Office of Record*)
CST	Centre de la sécurité des télécommunications
DG	Directeur général
DGSM	*Directive sur la gestion de la sécurité ministérielle*
DID	Description des données (*Data Item Description*)
É.-U.	États-Unis
ECMCC	Entente de contrôle du matériel COMSEC comptable
FSU	Mise à niveau logicielle sur le terrain (*Field Software Upgrade*)
GC	Gouvernement du Canada
HTTPS	Protocole HTTPS (*HyperText Transfer Protocol Secure*)
ICP	Infrastructure à clé publique
IMPC	Inspection des mesures de protection COMSEC
IP	En cours de réalisation (*In-Process*)
ITAR	*International Traffic in Arms Regulations*
ITSD	Directive en matière de sécurité des technologies de l'information (*Information Technology Security Directive*)
LGFP	*Loi sur la gestion des finances publiques*
LVERS	Liste de vérification des exigences relatives à la sécurité
MCC	Matériel COMSEC comptable
MSI	*Manuel de la sécurité industrielle*
NCOR	Bureau national des dossiers (*National Central Office of Record*)
NLZ	Zone jamais seul (*No-Lone Zone*)
OTAN	Organisation du traité de l'Atlantique nord
PCIE	Propriété, contrôle et influence de l'étranger
PMC	Programme des marchandises contrôlées
PSG	*Politique sur la sécurité du gouvernement*
PSI	Programme de sécurité industrielle
PUC	Portail de l'utilisateur COMSEC
PWA	Carte imprimée logique (*Printed Wiring Assembly*)
SNCMC	Système national de contrôle du matériel COMSEC
SPAC	Services publics et Approvisionnement Canada
TI	Technologies de l'information
TPI	Intégrité par deux personnes (*Two-Person Integrity*)
USML	United States Munitions List

11 Glossaire

Le présent glossaire contient la définition de certains termes ayant trait au matériel COMSEC faisant l'objet de la présente directive.

NON CLASSIFIÉ	
Accès	Capacité et possibilité de prendre connaissance ou de prendre possession d'une information ou d'un matériel, ou encore de modifier cette information ou ce matériel.
Accusé de réception	Document comptable (GC-223) servant à enregistrer la remise d'un matériel COMSEC et l'acceptation de la responsabilité du matériel remis.
Agent de sécurité de l'entreprise (ASE)	Personne-ressource officielle d'une entreprise du secteur privé auprès du PSI responsable de surveiller le profil de sécurité de l'entreprise et de régler les problèmes de sécurité, et devant rendre compte de toutes les questions de sécurité industrielle au PSI et au cadre supérieur clé de l'entreprise.
Agent de sécurité du ministère (ASM)	Personne chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme de sécurité du ministère qui soit conforme à la *Politique sur la sécurité du gouvernement* et aux normes qui s'y rattachent.
Article cryptographique contrôlé (CCI)	Système sécurisé d'information ou de télécommunications, ou composant cryptographique connexe, NON CLASSIFIÉ, mais régi par un ensemble spécial d'exigences en matière de contrôle au sein du SNCMC et portant la mention « article cryptographique contrôlé » (ou « CCI » lorsque l'espace est limité).
Autorité COMSEC du ministère (ACM)	Personne désignée par l'agent de sécurité du ministère et responsable, devant celui-ci, d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller un programme de sécurité des communications du ministère qui soit conforme à la *Politique sur la sécurité du gouvernement* et aux normes qui s'y rattachent.
Bureau national des dossiers (NCOR)	Entité du CST chargée de superviser la gestion et la comptabilité de tout le matériel COMSEC comptable produit au Canada ou confié à celui-ci.
Bureau national des incidents COMSEC (BNIC)	Entité du CST chargée de gérer les incidents liés à la sécurité des communications par l'enregistrement, la validation, l'évaluation et la fermeture des dossiers.
Centre d'assistance en matière de matériel cryptographique (CAMC)	Entité au sein du CST chargée de tous les aspects liés à la commande des clés, y compris la gestion des privilèges, et responsable de la gestion du Bureau national des dossiers et de l'administration du centre d'assistance.
Code de comptabilité (CC)	Code numérique servant à indiquer les contrôles de comptabilité minimaux auxquels sont assujettis les articles de matériel COMSEC au sein du SNCMS.

NON CLASSIFIÉ	
Compte COMSEC industriel du CST (CCIC)	Entité du CST chargée d'élaborer, de mettre en œuvre, de maintenir, de coordonner et de surveiller le programme de sécurité des communications d'une entreprise privée et d'en assurer la conformité à la *Politique sur la sécurité du gouvernement* et aux instruments de politique connexes aux fins de gestion du matériel COMSEC comptable.
Détenteur de prêt	Personne inscrite auprès d'un compte COMSEC ou d'un sous-compte COMSEC, qui est autorisée à recevoir du matériel COMSEC provenant du compte ou sous-compte en question.
Dispositif de gestion de palier 3 (T3MD pour *Tier 3 Management Device*)	Équipement cryptographique permettant de stocker, de transporter et de transférer (électroniquement) des clés cryptographiques en toute sécurité et pouvant être programmé pour appuyer les systèmes de mission modernes.
Équipe de vérification COMSEC à l'échelle nationale (EVCN)	Entité du CST chargée de mener les vérifications COMSEC des comptes COMSEC au sein du SNCMC.
Incident COMSEC	Tout événement qui met en péril ou pourrait mettre en péril la sécurité de renseignements classifiés ou protégés du GC pendant leur stockage, leur traitement, leur transmission ou leur réception
Intégrité par deux personnes (TPI)	Procédure selon laquelle les clés TRÈS SECRET et d'autres clés particulières ne doivent jamais être manutentionnées par une seule personne ou mises à la disposition d'une seule personne.
Matériel COMSEC	Matériel conçu pour sécuriser ou authentifier l'information de télécommunications. Le matériel COMSEC comprend, notamment, les clés, l'équipement, les modules, les dispositifs, les documents, le matériel informatique, les microgiciels ou logiciels qui comportent ou décrivent une logique cryptographique et d'autres articles qui exécutent des fonctions COMSEC.
Matériel COMSEC en cours de réalisation (IP)	Matériel COMSEC en cours de développement, de production, de fabrication ou de réparation. Voir « matériel COMSEC ».
Micrologiciel	Programmes et composants de données d'un module cryptographique qui sont stockés dans du matériel au sein du périmètre cryptographique et qui ne peuvent pas être écrits ou modifiés dynamiquement pendant l'exécution.
Ministère du gouvernement du Canada (GC)	Tout ministère, organisme, agence ou institution fédéral assujetti à la *Politique sur la sécurité du gouvernement*.
Parrain du gouvernement du Canada (GC)	Ministère du gouvernement du Canada qui a accepté de parrainer une entreprise du secteur privé autorisée à recevoir (aux fins d'utilisation), fabriquer, reproduire ou réparer du matériel COMSEC comptable et à y accéder.

NON CLASSIFIÉ	
Propriété, contrôle et influence étrangers (PCIE)	Situation en vertu de laquelle un tiers, une personne, une entreprise ou un gouvernement, est présumé avoir le contrôle d'une installation canadienne au point qu'un tiers, une personne, une entreprise ou un gouvernement, puisse accéder de façon non autorisée à des renseignements liés à la sécurité des technologies de l'information. Une détermination administrative de la nature et de la portée du contrôle étranger sur les opérations ou la gestion de l'entrepreneur est requise. On peut aussi dire « propriété étrangère » ou « contrôle étranger ».
Photomasque	Pellicule ou négatif sur verre, contenant de nombreuses images à haute résolution, utilisé dans la production de dispositifs à semi-conducteur et de circuits intégrés.
Responsabilité	Obligation d'une personne de protéger et de contrôler le matériel COMSEC qui lui a été confié.
Réticule	Disque ou objet semblable sur lequel alternent des parties opaques et transparentes et que l'on peut faire tourner devant un faisceau de lumière ou une autre source de rayonnement de façon à le moduler.
Secteur privé	Organisations, entreprises ou personnes du Canada qui ne sont pas assujetties à la *Loi sur la gestion des finances publiques* et qui ne relèvent pas d'un gouvernement provincial ou municipal.
Sécurité des communications (COMSEC)	Application de mesures de sécurité cryptographique, de sécurité des transmissions et des émissions, et de sécurité physique, ainsi que de pratiques et de mécanismes de contrôle opérationnels, visant à empêcher tout accès non autorisé à l'information issue de télécommunications et à garantir l'authenticité des télécommunications en question.
Sécurité des technologies de l'information (STI)	Mesures de protection visant à préserver la confidentialité, l'intégrité, la disponibilité, l'utilisation prévue et la valeur des renseignements conservés, traités ou transmis par voie électronique.
Sécurité physique	Mesures de protection physique visant à empêcher ou retarder l'accès non autorisé aux biens, à détecter l'accès non autorisé recherché et obtenu, et à déclencher une intervention appropriée.
Services à la clientèle en matière de COMSEC	Entité du CST chargée de fournir des conseils et une orientation au gouvernement du Canada ainsi qu'aux organismes parrainés du secteur privé canadien, en vue de la planification, de l'acquisition et de l'exploitation de matériel COMSEC, de services et de produits d'assurance élevée.
Système national de contrôle du matériel COMSEC (SNCMC)	Système centralisé, comprenant personnel, formation et procédures, qui permet aux ministères du gouvernement du Canada d'exercer un contrôle positif et d'effectuer un traitement efficace du matériel COMSEC comptable.
Tranche	Tranche mince d'un matériau semi-conducteur, comme un cristal de silicium, utilisée dans la fabrication de circuits intégrés et d'autres microdispositifs.

NON CLASSIFIÉ	
Vérification	Processus de revue et d'examen indépendants des enregistrements et des activités d'un système visant à tester l'adéquation des contrôles système, dans le but d'assurer la conformité aux politiques et aux procédures opérationnelles établies et de recommander les modifications qui s'imposent aux contrôles, aux politiques ou aux procédures.
Zone jamais seul	Secteur, pièce ou espace auquel personne ne peut accéder sans être accompagné et qui, lorsqu'il est occupé, doit l'être par deux ou plusieurs personnes conformément habilitées qui doivent demeurer en contact visuel constant l'une de l'autre.

12 Bibliographie

Les documents suivants ont servi à l'élaboration de la présente directive.

- **Centre de la sécurité des télécommunications**
  - *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC dans le secteur privé canadien* (ITSD-06A), 2016
  - *Directive en matière de sécurité des TI sur le contrôle du matériel COMSEC au sein du gouvernement du Canada* (ITSD-03A), mars 2014
  - *Directive sur l'utilisation de l'équipement COMSEC et des clés approuvés par le CSTC dans un réseau de télécommunication* (ITSD-04), novembre 2011
  - *Directive sur le signalement et l'évaluation des incidents COMSEC touchant le matériel COMSEC comptable* (ITSD-05), avril 2012
- **Ministère de la Justice**
  - *Loi sur la gestion des finances publiques* (LGFP), 1985
- **Services publics et Approvisionnement Canada**
  - *Manuel de la sécurité industrielle* (MSI), octobre 2014
- **Secrétariat du Conseil du Trésor**
  - *Directive sur la gestion de la sécurité ministérielle* (DGSM), juillet 2009
  - *Politique sur la sécurité du gouvernement* (PSG), juillet 2009