Catégorie 1150: Sécurité de l'information

Note 1 :
Le statut des équipements, du «logiciel», des systèmes, des «ensembles électroniques» spécifiques à une application donnée, des modules, des circuits intégrés, des composants ou des fonctions assurant la «sécurité de l'information» est déterminé dans la présente Catégorie, même s'il s'agit de composants ou d'«ensembles électroniques» d'autres équipements.

Note 2 :
La catégorie 1150. ne vise pas les produits lorsqu'ils accompagnent leur utilisateur aux fins d'usage personnel.

Note 3 :
Note sur la cryptologie
Les alinéas 1151. et 1154. ne visent pas les articles qui répondent à toutes les exigences suivantes :

a. généralement offerts au public en étant vendus, sans restriction à partir de stocks à des points de vente au détail par l'entremise des transactions suivantes :
   1. transactions au comptoir;
   2. transactions postales;
   *3. transactions électroniques; **ou***
   4. transactions téléphoniques;
b. la fonctionnalité de cryptologie ne peut pas être facilement modifiée par l'utilisateur;
c. conçus aux fins d'installation par l'utilisateur sans soutien significatif accru de la part du fournisseur;
*d. ne contient pas un «algorithme symétrique» faisant appel à une longueur de clé dépassant 64 bits; **et***
e. au besoin, les détails des articles sont accessibles et seront fournis, sur demande, à l'autorité appropriée dans le pays de l'exportateur afin de s'assurer de leur conformité aux conditions décrites aux alinéas a. à d. ci-dessus.
   N.B. :
   Les termes «autorité appropriée» s'entendent de toute agent de la Division du contrôle des exportations du ministère des Affaires étrangères et du Commerce international.

Note technique :
Dans la catégorie 1150., les bits de parité ne sont pas compris dans la longueur de clé.

1151. Systèmes, équipements et composants

1. Systèmes, équipements, «ensembles électroniques» spécifiques à une application donnée, modules ou circuits intégrés assurant la «sécurité de l'information», comme suit, et leurs autres composants spécialement conçus :
   N.B.
   Pour le statut des équipements de réception de positionnement global par satellite (GPS ou GNNS), voir le paragraphe 1071.5.

   a. conçus ou modifiés pour utiliser la «cryptologie» faisant appel à des techniques numériques assurant toute fonction cryptologique autre que l'authentification ou la signature numérique présentant l'une des caractéristiques suivantes :
      Notes techniques :
      1. Les fonctions d'authentification et de signature numérique comprennent leur fonction de gestion des clés connexe.
      2. l'authentification comprend tous les aspects de contrôle d'accès où il n'y a aucune cryptologie de fichiers ou de texte, exception faite des cas où la cryptologie est liée à la protection de mots de passe de numéros d'identification personnel (NIP) ou de toute donnée semblable afin de prévenir tout accès non autorisé.
      3. la «cryptologie» ne comprend pas les techniques de compression ou de codage de données «fixes».
         Note :
         L'alinéa 1151.1.a. comprend les équipements conçus ou modifiés pour utiliser la «cryptologie» faisant appel aux principes de l'analogie lorsqu'elle est mise en place avec les techniques numériques.
      1. un «algorithme symérique» faisant appel à une longueur de clé de plus de 56 bits; **ou**
      2. un «algorithme asymétrique» où la sécurité de l'algorithme est fondée sur l'une des caractéristiques suivantes :
         a. factorisation des nombres entiers de plus de 512 bits (p. ex. RSA);
         b. calcul des logarithmes discrets dans un groupe multiplicatif d'une dimension de champ supérieure à 512 bits (p. ex. Diffie-Hellman sur Z/pZ); **ou**
         c. logarithmes discrets dans un groupe différent de celui mentionné à l'alinéa 1151.1.a.2.b. de plus de 112 bits (p. ex. Diffie-Hellman sur une ellipse);
   b. conçus ou modifiés pour effectuer des fonctions cryptoanalytiques;
   c. spécialement conçus ou modifiés pour réduire les émanations compromettantes de signaux porteurs d'information, au-delà de ce qui est nécessaire dans le cadre des normes de santé, de sécurité ou de brouillage électromagnétique;
   d. conçus ou modifiés pour employer des techniques cryptologiques pour générer le code d'étalement pour le «spectre étalé» ou le code de saut pour les systèmes à «agilité de fréquence»;
   e. conçus ou modifiés pour assurer une «sécurité multiniveau» ou une isolation de l'utilisateur certifiées ou certifiables à un niveau dépassant la Classe B2 de la norme 'Trusted Computer System Evaluation Criteria' (TCSEC) ou d'une norme équivalente;
   f. systèmes de câbles de télécommunication conçus ou modifiés en faisant appel à des moyens mécaniques, électriques ou électroniques pour détecter les intrusions subreptices.

Note :
Le paragraphe 1151. ne vise pas ce qui suit :

a. «cartes à microprocesseur personnalisées» dans lesquelles la capacité de cryptologie est pour usage restreint dans des équipements ou des systèmes non visés par les alinéas b. à f. de la présente note.
   N.B. :
   Si une «carte à microprocesseurs personnalisée» présente de multiples fonctions, l'état de contrôle de chaque fonction est accédée individuellement.
b. équipements de réception pour la radiodiffusion, la télévision payante ou la télévision similaire réservée à un nombre limité de téléspectateurs, du type grand public, sans capacité de chiffrement numérique, exception faite du chiffrement utilisé exclusivement pour l'envoi de renseignements de facturation ou liés à des programmes à destination des fournisseurs de services de radiodiffusion;
c. équipements dans lesquels la capacité de cryptologie n'est pas accessible par l'utilisateur et qui sont spécialement conçus et limités pour respecter l'une des conditions suivantes :
   1. exécution de logiciels protégés contre la copie;
   2. accès à l'une des caractéristiques suivantes :
      a. support protégé contre la copie, en lecture seule; ou
      *b. renseignements stockés sous forme chiffrée sur support (p. ex. en rapport avec la protection des droits de propriété intellectuelle) lorsque le support est offert en vente au public dans des ensembles identiques; **ou***
   3. copie ponctuelle de données audio/vidéo protégées par le droit d'auteur.