Category 1150: Information Security

Note 1:
The control status of "information security" equipment, "software", systems, application specific "electronic assemblies", modules, integrated circuits, components or functions is determined in this Category even if they are components or "electronic assemblies" of other equipment.

Note 2:
Category 1150 does not control products when accompanying their user for the user's personal use.

Note 3:
Cryptography Note
1151. and 1154. do not control items that meet all of the following:

a. *Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:*
   1. *Over-the-counter transactions;*
   2. *Mail order transactions;*
   3. *Electronic transactions;* ***or***
   4. *Telephone call transactions;*
b. *The cryptographic functionality cannot easily be changed by the user;*
c. *Designed for installation by the user without further substantial support by the supplier;* ***and***
d. *When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. to c. above.*
   N.B.:
   The 'appropriate authority' means an officer of the Export Controls Division of the Department of Foreign Affairs and International Trade.

Technical Note:
In Category 1150., parity bits are not included in the key length.

1151. Systems, Equipment and Components

1. Systems, equipment, application specific "electronic assemblies", modules or integrated circuits for "information security", as follows, and other specially designed components therefore:
   N.B.:
   For the control of global navigation satellite systems receiving equipment containing or employing decryption (i.e., GPS or GLONASS), see 1071.5.

   a. Designed or modified to use "cryptography" employing digital techniques performing any cryptographic function other than authentication or digital signature having any of the following:
      Technical Notes:
      1. *Authentication and digital signature functions include their associated key management function.*
      2. *Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorised access.*
      3. *"Cryptography" does not include "fixed" data compression or coding techniques.*

      Note:
      1151.1.a. includes equipment designed or modified to use "cryptography" employing analogue principles when implemented with digital techniques.

      1. A "symmetric algorithm" employing a key length in excess of 56 bits; **or**
      2. An "asymmetric algorithm" where the security of the algorithm is based on any of the following:
         a. Factorization of integers in excess of 512 bits (e.g., RSA);
         b. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); **or**
         c. Discrete logarithms in a group other than mentioned in 1151.1.a.2.b. in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);
   b. Designed or modified to perform cryptanalytic functions;
   c. Deleted;
   d. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;
   e. Designed or modified to use cryptographic techniques to generate the spreading code for "spread spectrum" systems, including the hopping code for "frequency hopping" systems;
   f. Designed or modified to use cryptographic techniques to generate channelizing or scrambling codes for "time-modulated ultra-wideband" systems;
   g. Designed or modified to provide certified or certifiable "multilevel security" or user isolation at a level exceeding Class B2 of the Trusted Computer System Evaluation Criteria (TCSEC) or equivalent;
   h. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

   Note:
   1151. does not control:
   a. *"Personalised smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control under entries b. to f. of this Note. If a "personalised smart card" has multiple functions, the control status of each function is assessed individually.*
   b. *Receiving equipment for radio broadcast, pay television or similar restricted audience broadcast of the consumer type, without digital encryption except that exclusively used for sending the billing or programme-related information back to the broadcast providers;*
   c. *Equipment where the cryptographic capability is not user-accessible and which is specially designed and limited to allow any of the following:*
      1. *Execution of copy-protected software;*
      2. *Access to any of the following:*
         a. *Copy-protected contents stored on read-only media; or*
         b. *Information stored in encrypted form on media (e.g. in connection with the protection of intellectual property rights) when the media is offered for sale in identical sets to the public;* ***or***
      3. *One-time copying of copyright protected audio/video data.*
   d. *Cryptographic equipment specially designed and limited for banking use or money transactions;*
      Technical Note:
      'Money transactions' in 1151. Note d. includes the collection and settlement of fares or credit functions.
   e. *Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radiocommunications systems) that are not capable of end-to-end encryption;*
   f. *Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (i.e., a single, unrelayed hop between terminal and home basestation) is less than 400 metres according to the manufacturer's specifications.*

1152. Test, Inspection and Production Equipment

1. Equipment specially designed for:
   a. The "development" of equipment or functions controlled by Category 1150, including measuring or test equipment;
   b. The "production" of equipment or functions controlled by Category 1150, including measuring, test, repair or production equipment.