

“production” of equipment designed or modified for operation in any frequency band which is “allocated by the ITU” for radio-communications services, but not for radio-determination.

c.5. Equipment employing “common channel signaling” operating in non-associated mode of operation.

■ 29. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5—Telecommunications and “Information Security”, Part II—“Information Security”, Export Control Classification Number (ECCN) 5A002 is amended by revising the “Related Controls”, “Related Definitions”, and “Items” paragraphs in the List of Items Controlled section, to read as follows:

5A002 Systems, equipment, application specific “electronic assemblies”, modules and integrated circuits for “information security”, as follows (see List of Items Controlled), and other specially designed components therefor.

* * * * *

List of Items Controlled

Unit: * * *

Related Controls: 5A002 does not control the items listed in paragraphs (a) through (f) in the Note in the items paragraph of this entry. These items are instead controlled under ECCN 5A992.

Related Definitions: N/A

Items:

Note: 5A002 does not control the following. However, these items are instead controlled under 5A992:

(a) “Personalized smart cards”:

(1) Where the cryptographic capability is restricted for use in equipment or systems excluded from control paragraphs (b) through (f) of this Note; or

(2) For general public-use applications where the cryptographic capability is not user-accessible and it is specially designed and limited to allow protection of personal data stored within.

N.B.: If a “personalized 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 program-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) where the media is offered for sale in identical sets to the public; or

(3) Copying control of copyright protected audio/video data.

(d) Cryptographic equipment specially designed and limited for banking use or money transactions;

(e) Portable or mobile radiotelephones for civil use (e.g., for use with commercial civil cellular radio communications systems) that are not capable of end-to-end encryption.

N.B.: The term “money transactions” includes the collection and settlement of fares or credit functions.

(f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range of unboosted cordless operation (e.g., a single, unrelayed hop between terminal and home base station) is less than 400 meters according to the manufacturer’s specifications.

Technical Note: Parity bits are not included in the key length.

a. Systems, equipment, application specific “electronic assemblies”, modules and integrated circuits for “information security”, as follows, and other specially designed components therefor:

N.B.: For the control of global navigation satellite systems receiving equipment containing or employing decryption (e.g., GPS or GLONASS) see 7A005.

a.1. 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 unauthorized access.

3. “Cryptography” does not include “fixed” data compression or coding techniques.

Note: 5A002.a.1 includes equipment designed or modified to use “cryptography” employing analog principles when implemented with digital techniques.

a.1.a. A “symmetric algorithm” employing a key length in excess of 56-bits; or

a.1.b. An “asymmetric algorithm” where the security of the algorithm is based on any of the following:

a.1.b.1. Factorization of integers in excess of 512 bits (e.g., RSA);

a.1.b.2. 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

a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);

a.2. Designed or modified to perform cryptanalytic functions;

a.3. [RESERVED]

a.4. Specially designed or modified to reduce the compromising emanations of information-bearing signals beyond what is necessary for health, safety or electromagnetic interference standards;

a.5. Designed or modified to use cryptographic techniques to generate the

spreading code for “spread spectrum” systems, including the hopping code for “frequency hopping” systems;

a.6. Designed or modified to use cryptographic techniques to generate channelizing or scrambling codes for “time-modulated ultra-wideband” systems;

a.7. 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;

a.8. Communications cable systems designed or modified using mechanical, electrical or electronic means to detect surreptitious intrusion.

■ 30. In Supplement No. 1 to part 774 (the Commerce Control List), Category 6—Sensors, Export Control Classification Number (ECCN) 6A001 is amended by revising the License Exceptions section, and the “items” paragraph in the List of Items Controlled section, to read as follows:

6A001 Acoustics.

* * * * *

License Exceptions

LVS: \$3000; N/A for 6A001.a.1.b.1 object detection and location systems having a transmitting frequency below 5 kHz or a sound pressure level exceeding 210 dB (reference 1 μ Pa at 1 m) for equipment with an operating frequency in the band from 30 kHz to 2 kHz inclusive; 6A001.a.2.a.1, a.2.a.2, a.2.a.4, a.2.a.5, 6A001.a.2.b; processing equipment controlled by 6A001.a.2.c, and specially designed for real time application with towed acoustic hydrophone arrays; a.2.e.1, a.2.e.2; and bottom or bay cable systems controlled by 6A001.a.2.f and having processing equipment specially designed for real time application with bottom or bay cable systems.

GBS: Yes for 6A001.a.1.b.4.

CIV: Yes for 6A001.a.1.b.4.

List of Items Controlled

Unit: * * *

Related Controls: * * *

Related Definitions: * * *

Items:

a. Marine acoustic systems, equipment and specially designed components therefor, as follows:

a.1. Active (transmitting or transmitting-and-receiving) systems, equipment and specially designed components therefor, as follows:

Note: 6A001.a.1 does not control:

a. Depth sounders operating vertically below the apparatus, not including a scanning function exceeding $\pm 20^\circ$, and limited to measuring the depth of water, the distance of submerged or buried objects or fish finding;

b. Acoustic beacons, as follows:

1. Acoustic emergency beacons;

2. Pingers specially designed for relocating or returning to an underwater position.

a.1.a. Wide-swath bathymetric survey systems designed for sea bed topographic mapping, having all of the following: