

b.3. "Technology" for the "development" of digital cellular radio base station receiving equipment whose reception capabilities that allow multi-band, multi-channel, multi-mode, multi-coding algorithm or multi-protocol operation can be modified by changes in "software"

b.4. "Technology" for the "development" of "spread spectrum" techniques, including "frequency hopping" techniques.

c. "Technology" according the General Technology Note for the "development" or "production" of any of the following telecommunication transmission or "stored program controlled" switching equipment, functions or features:

c.1. Equipment employing digital techniques, including "Asynchronous Transfer Mode" ("ATM"), designed to operate at a "total digital transfer rate" exceeding 1.5 Gbit/s;

c.2. Equipment employing a "laser" and having any of the following:

c.2.a. A transmission wavelength exceeding 1750 nm;

c.2.b. Performing "optical amplification" using praseodymium-doped fluoride fiber amplifiers (PDFFA);

c.2.c. Employing coherent optical transmission or coherent optical detection techniques (also called optical heterodyne or homodyne techniques);

c.2.d. Employing wavelength division multiplexing techniques exceeding 8 optical carriers in a single optical window; or

c.2.e. Employing analog techniques and having a bandwidth exceeding 2.5 GHz;

**Note:** 5E001.c.2.e. does not control "technology" for the "development" or "production" of commercial TV systems.

c.3. Equipment employing "optical switching";

c.4. Radio equipment having any of the following:

c.4.a. Quadrature-amplitude-modulation (QAM) techniques above level 128; or

c.4.b. Operating at input or output frequencies exceeding 31 GHz; or

**Note:** 5E001.c.4.b. does not control "technology" for the "development" or "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 either non-associated or quasi-associated mode of operation.

**5E991 "Technology" for the "development", "production" or "use" of equipment controlled by 5A991 or 5B991, or "software" controlled by 5D991, and other "technologies" as follows (see List of Items Controlled).**

\* \* \* \* \*

#### List of Items Controlled

Unit: \* \* \*

Related Controls: \* \* \*

Related Definitions: (1) "Synchronous digital hierarchy" (SDH) is a digital hierarchy providing a means to manage, multiplex, and access various forms of digital traffic using a

synchronous transmission format on different types of media. The format is based on the Synchronous Transport Module (STM) that is defined by CCITT Recommendation G.703, G.707, G.708, G.709 and others yet to be published. The first level rate of 'SDH' is 155.52 Mbits/s. (2) 'Synchronous optical network' (SONET) is a network providing a means to manage, multiplex and access various forms of digital traffic using a synchronous transmission format on fiber optics. The format is the North America version of 'SDH' and also uses the Synchronous Transport Module (STM). However, it uses the Synchronous Transport Signal (STS) as the basic transport module with a first level rate of 51.81 Mbits/s. The SONET standards are being integrated into those of 'SDH'.

#### Items:

a. Specific "technologies" as follows:

a.1. "Technology" for the processing and application of coatings to optical fiber specially designed to make it suitable for underwater use;

a.2. "Technology" for the "development" of equipment employing 'Synchronous Digital Hierarchy' ('SDH') or 'Synchronous Optical Network' ('SONET') techniques.

13. In Supplement No. 1 to part 774 (the Commerce Control List), Category 5—Telecommunications and "Information Security", Part II—"Information Security" is amended by:

(a) Revising the Heading and the *Related Controls* paragraph and the *Items* paragraph in the List of Items Controlled section of ECCN 5A002, to read as set forth below; and

(b) Amending the License Requirements section of ECCNs 5B002 and 5E002 by removing the *License Requirements Notes* paragraph at the end of this section.

**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: See also 5A992. This entry does not control:

(a) "Personalized smart cards" where the cryptographic capability is restricted for use in equipment or systems excluded from control paragraphs (b) through (f) of this note. Note that 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) 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;

(d) 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) one-time encryption of copyright protected audio/video data;

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

(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 basestation) is less than 400 meters according to the manufacturer's specifications. These items are controlled under ECCN 5A992.

Related Definitions: \* \* \*

#### Items:

**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", and other specially designed components therefor:

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