

Deloitte.

Encryption Overview



Deloitte Tax LLP
Customs & Global Trade

Agenda

Encryption Overview

Topic

Foundation of Export Controls

Overview of Encryption

What are Encryption Items?

How is Encryption Hardware and Software Controlled?

Overview of ECCN 5A002

Overview of Category 5, Part II Notes (1) – (4)

Questions

Appendix

Overview of Encryption

Introduction

What is Cryptography?

- The process of scrambling data to hide its content
- A critical technology for protecting valuable or sensitive information from unauthorized disclosure
- A staple feature of mainstream computer technology and electronic commerce
- Strictly controlled for national security and law enforcement reasons
- Incremental changes to U.S. and global export controls over the last two decades

Background

- Since ancient times, cryptography has been used to hide the contents of a message from adversaries.



Overview of Encryption

What is Encryption?

- Encryption is the process of encoding messages or information in such a way that only authorized parties may read it.

What is Cryptography?

- The means and methods for transformation of data in order to hide its information content, prevent undetected modification or prevent its unauthorized use.
- Products are controlled because of the capability to encrypt data, regardless of other functions and features. Encryption products can be hardware *or* software.
- Encrypted data is *not* controlled. The regulations do not control encrypted data for the sake of it being encrypted. This includes files, music, multimedia information, and video.
- The regulations do *not* consider compression to be cryptography.

Overview of Encryption

Why Controlled?

- Protect national security
- Preserve U.S. technology advantage
- Previously controlled under the ITAR

How Controlled?

- Controlled by the U.S. Department of Commerce, Bureau of Industry & Security (unless specifically designed for military/space application)
- Export Administration Regulations (EAR)
 - Commerce Control List, Part 774 Supplement No. 1
 - Category 5, Part II (“Information Security”)

U.S. National Encryption Controls

Encryption Items Subject to Control

Items **subject** to US encryption controls include:

- Products designed or modified to use cryptography or which contains encryption
- Products with the capability to encrypt data, regardless of other functions and features
- Products that contain encryption, even if the item does not use the encryption
- Products that utilize encryption from an external source, such as:
 - OS software
 - External/ESSL library
 - 3rd party product
 - Cryptographic processor
- Encryption products specially designed or modified for military use



U.S. National Encryption Controls

Encryption Items **NOT** Subject to Control

Items **not subject** to US encryption controls include:

- Products with dormant encryption that require cryptographic activation (the activation key for these products are controlled as encryption items, however)
- Products for mass market distribution
- Products that use encryption solely for:
 - Authentication and access control
 - Digital signature
 - Execution of copy-protected software
- Low-level encryption (\leq 56-bit symmetric encryption algorithm)
 - *Symmetric-key algorithms are algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical or there may be a simple transformation to go between the two keys*



U.S. National Encryption Controls

Encryption Items **NOT** Subject to Control

- Items “specially designed” for medical end-use
- Items for personal use or tools of trade eligible for TMP or BAG
- 5A002 and 5D002 do **not** control items that meet all of the below criteria:
 - 1) Available to the public by being sold without restriction from retail stock via:
 - a) Over-the-counter transactions
 - b) Mail order transactions
 - c) Electronic transactions
 - d) Telephone call transactions
 - 2) Cryptographic functionality cannot be easily manipulated by the user
 - 3) Designed for installation by the user without substantial support by the supplier
 - 4) (Technical) details available upon request to authority in exporter country

Note: item must also: (1) span interest over a wide range of individuals/businesses; (2) readily available price and information.



What are Encryption Items?

The Bureau of Industry and Security (Department of Commerce) controls encryption software, hardware, and technology but also what are referred to as '**Encryption Items**'.

Encryption items—includes all encryption commodities, software, and technology that contain encryption features and are subject to the EAR. Encryption items may either contain cryptography or may be designed to use cryptography.

Examples of Encryption Items:

- Electronics
- Computers
- Software
- Communications Equipment
- Storage Devices (e.g., Thumb drives, Flash Memory, Smart Cards)
- Wireless Devices (e.g., Bluetooth, Wi-Fi, IEEE 802.11)
- Wired Networking Devices
- Networking Equipment (routers/switches/base stations)



What are Encryption Items?

A hardware device or a software application may be considered an encryption when:

- Encryption functions are implemented by the device's electronics or firmware; or
- Encryption functions are implemented by the software's programming code; or
- When a the device or software merely 'calls upon' encryption functionality in another application (e.g., operating system software, external libraries, third party products or cryptographic processors).
- A device or software contains encryption that is not used but enabled.

Encryption 'Hot' Words

- WiFi
- TCP/IP
- IEEE 802.11
- Advanced Encryption Standard (AES)
- Diffie-Hellman
- Digital Signature Standard (DSS)
- Elliptical Curve
- BlowFish
- Rivest, Shamir and Adleman (RSA)
- Secure Socket Layer (SSL)
- Bluetooth



Reasons for Control

5A002



The “Controls” header identifies all applicable Reasons for Control, in order of restrictiveness and to what extent each applies. 5A002 is controlled for NS, AT and EI which apply to entire entry.

National Security

Controlled under NS, Column 1. 5A002 classified items require a license to all destinations except Canada. Certain exports may be eligible for a License Exception.

Anti-Terrorism

Controlled under AT, Column 1. 5A002 classified items require a license if exported to Cuba, Iran, North Korea, Sudan and Syria. No license exceptions apply.

Encryption Items

Exports and reexports of encryption software, like exports and reexports of encryption hardware, are controlled because of this functional capacity to encrypt information, and not because of any informational or theoretical value that such software may reflect, contain, or represent, or that its export or reexport may convey to others abroad.



How are Encryption Hardware Items Controlled?

If an item is determined to be an 'encryption item' and not exempt from classification in Category 5 Part 2 there are two possible Export Control Classification Numbers (ECCNs) that regulate hardware.

5A002	"Information Security" systems, equipment and "components" therefor, as follows (see List of Items Controlled)
	Reasons for Control: NS1, AT1, EI
	This ECCN requires a license for every destination except Canada
5A992	Equipment not controlled by 5A002 (see List of Items Controlled)
	Reasons for Control: AT1
	This ECCN only requires a license for the following countries: Cuba, Iran, Syria, North Korea and Sudan

Note: ECCN 5A002 is highly regulated and may only be exported to Canada without an export authorization. While 5A992 is controlled at a very low level.

How are Encryption Software Items Controlled?

If a software item is determined to be an 'encryption item' and not exempt from classification in Category 5 Part 2 there are two possible Export Control Classification Numbers (ECCNs) that regulate software.

5D002	"Software" as follows (see List of Items Controlled)
	Reasons for Control: NS1, AT1, EI
	This ECCN requires a license for every destination except Canada
5D992	"Information Security" "software" not controlled by 5D002 as follows (see List of Items Controlled)
	Reasons for Control: AT1
	This ECCN only requires a license for the following countries: Cuba, Iran, Syria, North Korea and Sudan

Note: ECCN 5D002 is highly regulated and may only be exported to Canada without an export authorization. While 5D992 is controlled at a very low level.

Overview of 5A002 & Exclusions

ECCN 5A002

Demystifying 5A002: When you strip away the (a) – (j) exclusions (discussed on next slide), 5A002 is actually fairly concise:

a. Systems, equipment and components, for “information security”, as follows:

a.1. Designed or modified to use “cryptography” employing digital techniques performing any cryptographic function other than authentication, digital signature, or execution of copy-protected “software,” and having any of the following:

- 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 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. [Reserved]

b. Designed or modified to enable, by means of “cryptographic”, an item to achieve or exceed the controlled performance levels for functionality specified by 5A002.a that would not otherwise be enabled

c. Designed or modified to use or perform “quantum cryptography”

d. Designed or modified to use cryptographic techniques to generate channelizing codes, scrambling codes or network identification codes, for systems using ultra-wideband modulation techniques and having any of the following:

- d.1. A bandwidth exceeding 500 MHz; or
- d.2. A “fractional bandwidth” of 20% or more;

e. Designed or modified to use cryptographic techniques to generate the spreading code for “spread spectrum” systems, not controlled in 5A002.d., including the hopping code for “frequency hopping” systems.

TECHNICAL NOTE:

1. Functions for authentication, digital signature and the execution of copy-protected “software” 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.

TECHNICAL NOTE: Parity bits are not included in the key length.cc

NOTE: 5A002 DOES NOT CONTROL ANY OF THE FOLLOWING: (SEE NEXT SLIDE)

TECHNICAL NOTE: “Quantum cryptography” is also known as Quantum Key Distribution (QKD).

ECCN 5A002 Exclusions

The introductory notes to ECCN 5A002 specifically exclude a number of items from classification under ECCN 5A002 (designated as (a) – (j)). The following items are excluded, and likely classifiable instead under EAR99.

1

- Certain Smart Cards

2

- Smart Card Reader/Writers

3

- Cryptographic equipment specially designed and limited for banking use or 'money transactions

4

- Portable or mobile radiotelephones for civil use

5

- Cordless telephone equipment not capable of end-to-end encryption

6

- Certain wireless "personal area network" equipment

7

- Encryption items limited to authentication
- Publicly available encryption source code

8

- Mobile telecommunications Radio Access Network (RAN) equipment designed for civil use

9

- General purpose computing equipment or servers, where the "information security" functionality meets certain standards

10

- Certain routers, switches or relays, where the "information security" functionality is limited to the tasks of "Operations, Administration or Maintenance"

- *[Deloitte note: Essentially, you have a general purpose computer or server where the encryption functionality is inside of a mass market processor, then this decontrol note could apply. Or if the encryption functionality is inside of just the operating system, that is a mass market operating system, then the decontrol could apply].*

Overview of 5A003, 5A004 & 5A992

New ECCNs to Category 5 part 2

5A003 & 5A004

5A003

“Systems,”

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

NOTE: 5A003.a applies only to physical layer security.

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

Formerly
under
5A002

5A004

“Systems,” “equipment” and “components” for defeating, weakening or bypassing “information security,” as follows

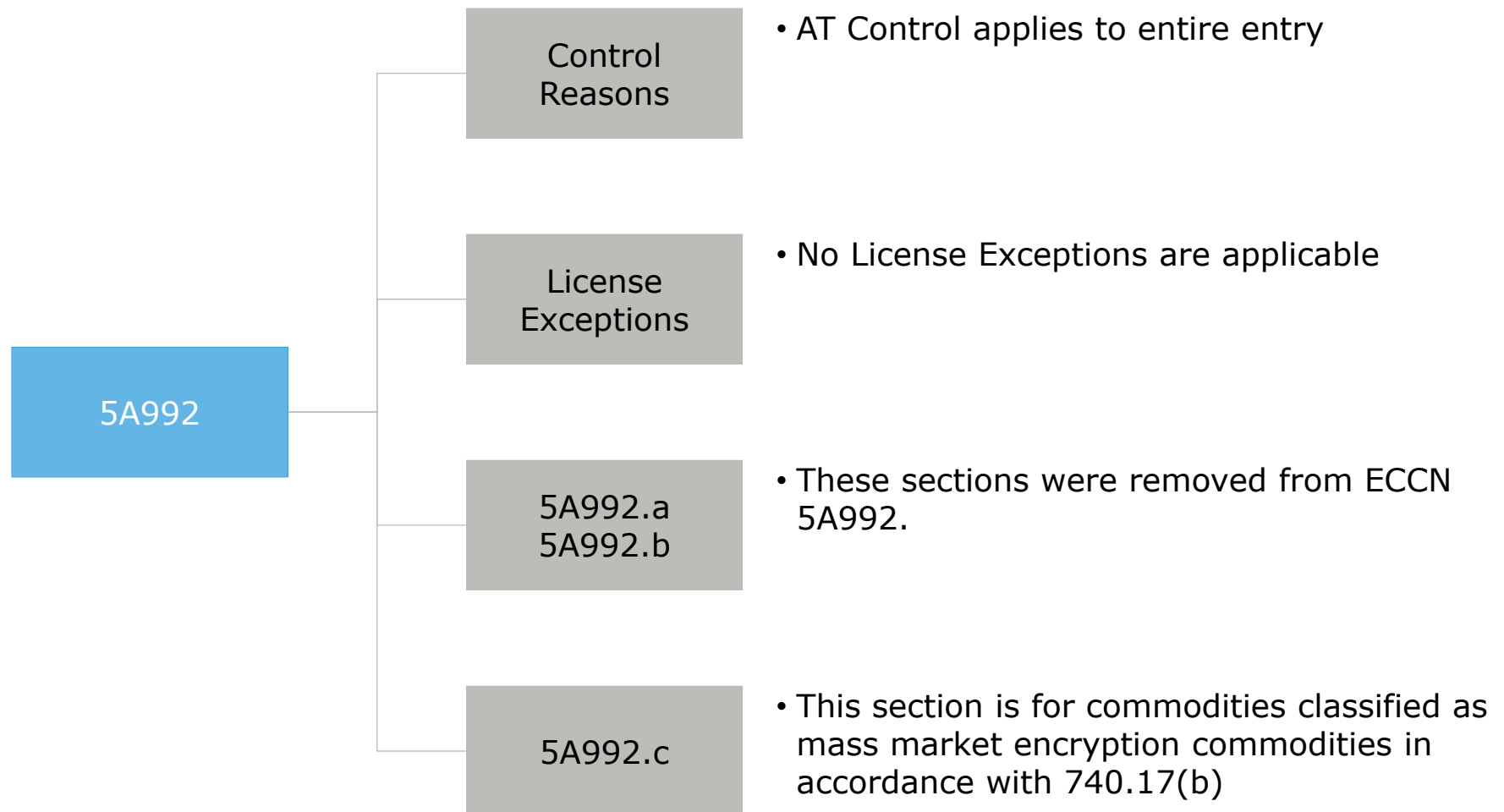
- a. Designed or modified to perform 'cryptanalytic functions.'

Note: 5A004.a includes systems or equipment, designed or modified to perform 'cryptanalytic functions' by means of reverse engineering.

Technical Note: 'Cryptanalytic functions' are functions designed to defeat cryptographic mechanisms in order to derive confidential variables or sensitive data, including clear text, passwords or cryptographic keys.

- b. [Reserved]

5A992 Updates



Category 5 Part 2 Notes

Encryption: Cat 5 Part 2

Category 5, Part 2

Introductory text

Note 1:

[Reserved]

Note 2:

Relates to license exceptions. Don't worry about it

Note 3:

Removes ECCNs 5A002, 5A003, 5A004 and 5D002 control items that qualify for "mass market"

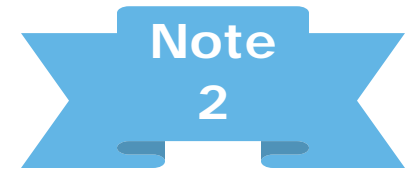
Once mass market registration is submitted by the manufacturer, the product will be classified in 5A992.c.

We can make reasonable assumptions, but best to confirm with manufacturer or classify 5A002 (vice 5A992.c), if we don't know whether registration has been submitted.

Note 4:

Encryption products meeting certain functions listed in this Note are COMPLETELY removed from Category 5 part 2 (but may be classified elsewhere)

Encryption: Cat 5 Part 2, Note 2

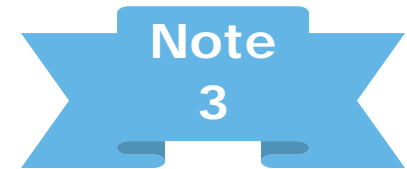


NOTE 2: Category 5, part 2, encryption products, when accompanying their user for the user's personal use or as tools of trade, are eligible for License Exceptions TMP or BAG, subject to the terms and conditions of these License Exceptions.

Discuss: What does this Note mean?

Encryption: Cat 5 Part 2, Note 3

Mass Market



NOTE 3: Cryptography Note: ECCNs 5A002, 5A003, 5A004 and 5D002 do not control items as follows:

a. Items meeting **all** of the following:

1. Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:

- a. Over-the-counter transactions;
- b. Mail order transactions;
- c. Electronic transactions; or
- d. Telephone call transactions;

This is known as the mass market provision

2. The cryptographic functionality cannot be easily changed by the user;

3. Designed for installation by the user without further substantial support by the supplier; and

4. [Reserved]

5. 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 1. through 3. of this Note a.;

Encryption: Cat 5 Part 2, Note 3

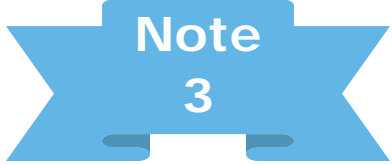
Mass Market

b. Hardware components or 'executable software', of existing items described in paragraph a. of this Note, that have been designed for these existing items, and meeting all of the following:

1. "Information security" is not the primary function or set of functions of the component or 'executable software';
2. The component or 'executable software' does not change any cryptographic functionality of the existing items, or add new cryptographic functionality to the existing items;
3. The feature set of the component or 'executable software' is fixed and is not designed or modified to customer specification; and
4. When necessary, as determined by the appropriate authority in the exporter's country, details of the component or 'executable software', and details of relevant end-items are accessible and will be provided to the authority upon request, in order to ascertain compliance with conditions described above

Technical Note: For the purpose of the Cryptography Note, 'executable software' means "software" in executable form, from an existing hardware component excluded from 5A002, 5A003, or 5A004 by the Cryptography Note.

Note: 'Executable software' does not include complete binary images of the "software" running on an end-item.



Note
3

Encryption: Cat 5 Part 2, Note 3

Mass Market

To meet paragraph a. of Note 3, all of the following must apply:

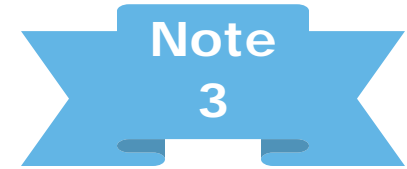
- a. The item is of potential interest to a wide range of individuals and businesses; *and*
 - b. The price and information about the main functionality of the item are available before purchase without the need to consult the vendor or supplier. A simple price inquiry is not considered to be a consultation.
2. In determining eligibility of paragraph a. of Note 3, BIS may take into account relevant factors such as quantity, price, required technical skill, existing sales channels, typical customers, typical use or any exclusionary practices of the supplier.

N.B. TO NOTE 3 (CRYPTOGRAPHY NOTE): You must submit a classification request or encryption registration to BIS for mass market encryption commodities and software eligible for the Cryptography Note employing a key length greater than 64 bits for the symmetric algorithm (or, for commodities and software not implementing any symmetric algorithms, employing a key length greater than 768 bits for asymmetric algorithms or greater than 128 bits for elliptic curve algorithms) in accordance with the requirements of §740.17(b) of the EAR in order to be released from the “EI” and “NS” controls of ECCN 5A002 or 5D002.

To be considered Mass Market, the item should first meet the criteria listed in Note 3 to Category 5, Part 2

Encryption: Cat 5 Part 2

Mass Market: Note 3

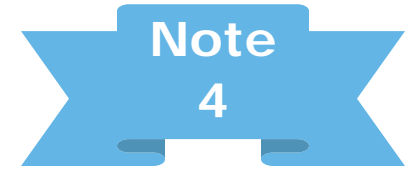


Mass market encryption products include, but are not limited to,

- General purpose operating systems and desktop applications (e.g., e-mail, browsers, games, word processing, database, financial applications or utilities) designed for use with computers classified as ECCN 4A994 or designated as EAR99;
- Laptops, or hand-held devices;
- Commodities and software for client Internet appliances and client wireless LAN devices;
- Home use networking commodities and software (e.g., personal firewalls, cable modems for personal computers, and consumer set top boxes);
- Portable or mobile civil telecommunications commodities and software (e.g., personal data assistants (PDAs), radios, or cellular products).

Encryption: Cat 5 Part 2, Note 4

Category 5, Part 2

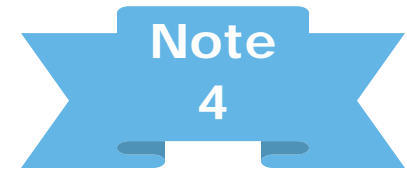


Note 4 Removes from the controls of Category 5 Part 2 any item where the **primary function or set of functions is NOT any of the following:**

- Information Security
- A computer, including operating systems, parts and components therefor
- Sending, receiving, or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records); or
- Networking (includes operation, administration, management and provisioning)



Note 4 Exclusion Examples

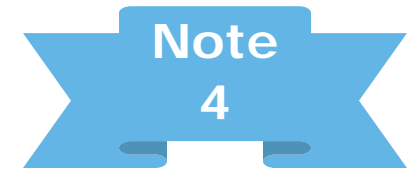


BIS has provided an illustrative list of items potentially covered by Note 4. The items include:

Consumer applications:

- Piracy and theft prevention for software or music
- Copyright protection
- Music/movies, digital photos/recorders
- Games/gaming – devices, runtime software, HDMI and other component interfaces, development tools
- LCD TV, Blu-ray, DCD, DVR, cinema, HDMI and other component interfaces (not videoconferencing)
- Printers, copiers, scanners, digital cameras, Internet cameras, including parts and subassemblies
- Household utilities and appliances

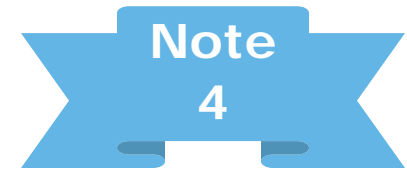
Note 4 Exclusion Examples



Business/systems applications: systems operations, integration and control:

- Business process automation – process planning and scheduling, supply chain management, inventory and delivery
- Transportation – safety and maintenance, systems monitoring and on-board controllers (including aviation, railway, and commercial automotive systems), 'smart highway' technologies, public transit operations and fare collection, etc.
- Industrial, manufacturing or mechanical systems – including robotics, plant safety, utilities, factory and other heavy equipment, facilities systems controllers such as fire alarms and HVAC
- Medical/Clinical – including diagnostic applications, patient scheduling, and medical data records confidentiality
- Applied geosciences – mining/drilling, atmospheric sampling/weather monitoring, mapping/surveying, dams/hydrology

Note 4 Exclusion Examples



Research/Scientific/analytical:

- Business process management – business process abstraction and modeling
- Scientific visualization/simulations/co-simulation (excluding such tools for computing, networking cryptanalysis, etc.) – process planning and scheduling, supply chain management, inventory and delivery
- Data synthesis tools for social, economic, and political sciences (e.g., economic, population, global climate change, public opinion polling, etc. forecasting and modeling).

Secure intellectual property (IP) delivery and installation:

- Software download auto-installers and updaters
- License key product protection and similar purchase validation
- Software and hardware design IP protection
- Computer aided design software and other drafting tools

Example for application of Note 4

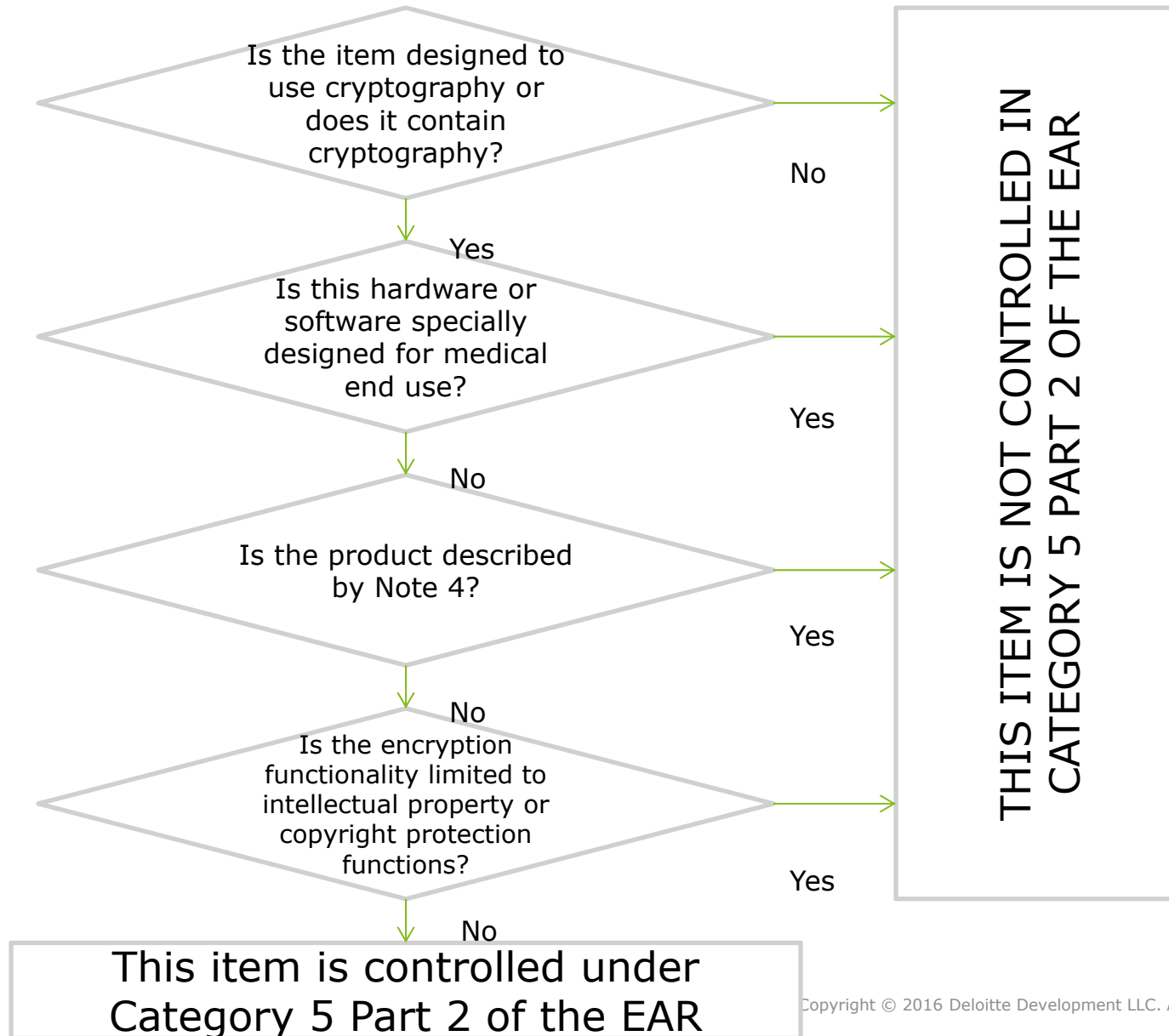
Example:

We have a connected home with lighting controls that are managed from your phone, (you have an app on your phone that is used to control the lights in your home). The data going from your phone to the lights are encrypted. You are using secure communications.

Does the app on your phone that is being used to control the lighting in your home, qualify for Note 4?

What about the phone itself?

Encryption Flow Chart



Questions?



Appendix



Official Professional Services Sponsor

Professional Services means audit, tax, consulting, and advisory.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a detailed description of DTTL and its member firms. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Copyright © 2016 Deloitte Development LLC. All rights reserved.
36 USC 220506

Overview of Encryption

A Primer on Cryptography

Key Crypto Terms & Concepts

- **Encryption** = scrambling the message
- **Decryption** = descrambling the message
- **Cryptographic Algorithm (or Cipher)** = mathematical function used for (de)encryption
- **Key** = string of bits (1's and 0's) to secure the message
- **Authentication** = encryption protocol that ensures a message is really from the sender

Secret-Key and Public-Key Encryption

Two main types of modern cryptographic systems:

- **Secret-key** = sender (encryption) and receiver (decryption) keys are the same; requires a trusted method for distributing keys
- **Public-key** = sender's "public key" and receiver's "private key" are inversely related and form a matched pair; used for "key exchange"

Crypto Key Lengths

- Key lengths in modern encryption can reach up to 3,072-bits (back in 2000 the longest key length was 128-bits).
- The shorter the key length, the more vulnerable a message is to attacks.

Crypto Algorithms

- Variations of DES and RSA are most popular for commercial use
- RC2 and RC4 are most popular for secret-key
- Diffie-Hellman and RSA are most popular public-key

PGP (Pretty Good Privacy) Software

- Well known crypto software program available to the public