



Encryption Export Controls

Judith Currie
Information Technology Controls Division
Bureau of Industry and Security
U.S. Department of Commerce
August 20, 2013
Arlington, Virginia



Encryption Export Controls Agenda

- What is and what is not an Encryption Item
- Encryption items with limited Encryption Controls
- Types of Export Authorizations for Encryption
 - License Exception ENC
 - Mass Market including June 20 Mass Market changes



Uses of Encryption

- Wired and wireless communications
- Open source and commercial software
- Components
- Stored data
- Data transfer
- Virtual Private Network (VPN)
- Operations, Administration, Maintenance and Provisioning (OAM&P)
- Access Control
- Copyright protection
- Financial transactions



Things to look for

- **Algorithms**

- Advanced Encryption Standard (AES)
- Rivest, Shamir, and Adleman (RSA)
- Data Encryption Standard (DES)
- Elliptic Curve Cryptography



- **Protocols**

- IP Security (IPSec)
- Secure Socket Layer (SSL)
- WiFi (IEEE 802.11) /
WiMAX (IEEE 802.16)



What's Your ECCN?

- Controlled for EI, NS and AT reasons:
 - 5A002 : hardware
 - 5D002 : software
 - 5E002 : technology
- Controlled for NS and AT reasons:
 - 5B002: test equipment
- Controlled for AT reasons only:
 - 5A992 : hardware
 - 5D992 : software
 - 5E992 : technology
- EAR99



Do I have an encryption item?

- As a general rule, Yes, if your item contains encryption.
 - Yes, even if your item does not use the encryption.
- Yes, if your item is designed to use encryption from an external source. Such as:
 - The operating system (OS) software
 - An external library
 - A third-party product
 - A cryptographic processor

Encryption Items

- Export of any item from the United States
- Reexport of U.S. origin items
- Foreign-made products incorporating greater than de minimis U.S. controlled content
- Foreign-made direct product of U.S. origin technology



How is encryption export control different?

- Transferred from DOS control in 1996 and retains elements of ITAR such as the “see thru rule”
- Export of encryption defined differently in 734.2(b)(9)
 - Software (including source code) transferred within the U.S. are not exports. (or deemed exports)
 - Making available for download is an export
 - Precautions required for export of software described by 740.17(b)(2)



Items Using Encryption NOT Controlled under Category 5, Part 2



Items using encryption not controlled in Category 5 Part 2

- Publicly Available items not subject to the EAR
- Note 1 NB items (medical end use)
- Note 4 items

Publicly available (free) object code using encryption

When is it 'not subject to the EAR'?

- Subject to the following changes made on January 7, 2011 such software can be 'not subject to the EAR'
 - If the source is TSU or
 - Even if the source is not TSU, after you follow all the registration and self-classification steps discussed earlier and register and self-classify as 5D992 because it is free to everyone and meets the publicly available tests

Medical devices: NOT ENCRYPTION

Medical devices are not subject to encryption controls



N.B. to Note 1: Medical end-use

- **Note 1:** *The control status of “information security” equipment, “software”, systems, application specific “electronic assemblies”, modules, integrated circuits, components, or functions is determined in Category 5, Part 2 even if they are components or “electronic assemblies” of other equipment.*
- N.B. to Note 1: Commodities and software specially designed for medical end-use that incorporate an item in Category 5, part 2 are not classified in any ECCN in Category 5, part 2

Note 4 to Category 5 Part 2

- Added in June 2010
- It excludes many items from Category 5 Part 2 based on their functionality.
- If Note 4 applies, the ECCN of the item is the ECCN it would be without encryption.
- If the item it is not described elsewhere in the CCL its ECCN is EAR99
- Note 4 overrides other reasons for decontrol
- Even overrides need for Note 3
- Interpreting Note 4 is difficult

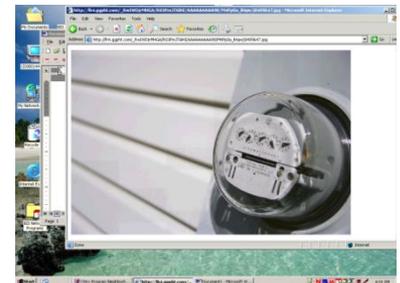
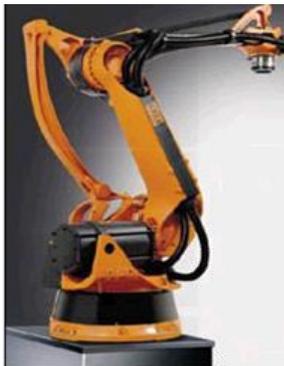
Applying Note 4 to determine whether an item is described in Category 5 Part 2

- Category 5 Part 2 includes only items that have any of the following ‘primary function’(s):
 - “Information security”
 - Computing
 - Communications
 - Networking
- provided that
- Encryption is limited to supporting the item’s primary function(s)
 - Details of encryption will be made available upon request

Note 4 Items

“Ancillary Cryptography”

- No Registration, No Review Required, No Reporting
- not primarily useful for computing (including the operation of "digital computers"), communications, networking (includes operation, administration, management and provisioning) or "information security".



Note 4 - Examples of Items excluded from Encryption Controls by Note 4

- Piracy and theft prevention for software, music, etc.
- Games and gaming (except communication games)
- Printing, reproduction, imaging and video recording or playback—not videoconferencing
- Business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery)
- Automotive, aviation, and other transportation systems

Note 4 - Examples of Items excluded from Encryption Controls by Note 4 (cont'd)

- Industrial, manufacturing or mechanical systems (e.g., robotics, heavy equipment, facilities systems such as fire alarm, HVAC)
- Mining, drilling, mapping products
- Household utilities and Household appliances
- Printers, copiers and digital cameras (not encrypted fax)
- Product where encryption is limited to copyright/ IP protection

Encryption Items controlled under Category 5, Part 2



Items using Encryption with Limited Encryption Controls

- Items exempt from encryption registration, classification and reporting requirements
 - Items described in ECCN 5A002 decontrol notes
 - Where encryption is limited to authentication only
 - Items limited to low-strength crypto
- Encryption exports eligible for automatic license exception (Items that can be exported to certain end-users or for certain end-uses under License Exception provisions.)
 - Note 2 exports (TMP and BAG)
 - ENC automatic License Exception provisions
 - Other automatic License Exception provisions (TMP *, BAG, GOV, LVS, RPL, TSU*)

NOTES TO CATEGORY 5 PART 2

Cat 5 Part 2 items controlled as 5x992 but not controlled under
ECCN 5X002

- Related controls -decontrol notes
 - authentication/digital signature
 - low-strength encryption
-
- These items are controlled for anti-terrorism reasons only under ECCN 5A992/5D992

Encryption products described by ECCN 5A002 decontrol notes (a)-(j)

- May be self-classified as 5A992-no registration
 - Examples –
 - Personalized **smart cards** and smart card **readers** (incl RFID)
 - Equipment specially designed for money transactions or banking use (finance specific)
 - Certain telephone equipment (including wireless telephones without end-to-end encryption)
 - client wireless devices (e.g. utility meter readers)
 - Wireless “personal area network” (**PAN**) equipment
 - *that implement only published or commercial cryptographic standards and*
 - *where the per manufacturers ‘specifications cryptographic capability is limited to a nominal operating range not exceeding 30 meters or not exceeding 100 meters for equipment that cannot interconnect with more than seven devices*
 - Equipment with encryption functionality that cannot be used
 - copyright protection and more - now in Note 4
 - Decontrol note (j) to ECCN 5A002

No Review Required, No Reporting: Wireless PAN Related Control Note

“Personal Area Network” items – arbitrary number of interconnected 'data devices' communicating directly with each other; and confined to immediate vicinity of an individual person or device controller (e.g., single room, office, or automobile).

- *nominal operating range \leq 30 meters or 100 meters for equipment that cannot interconnect with more than seven devices*

- 802.15.1: ask potential range
- May Self Classify as 5x992



AUTHENTICATION ONLY

- a.1. Designed or modified to use “cryptography” employing digital techniques performing **any cryptographic function other than authentication or digital signature . . .**
 - 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.
 - **Key words**
 - **Authentication**
 - **password protection**
 - **digital signature**

LOW-STRENGTH CRYPTO

(self-classify without registration when key lengths are equal to less than those specified below)

- Encryption items can be self-classified as 5A992 unless
 - 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);
- Mass Market Encryption items can be self-classified as 5A992 unless employing a key length greater than **64 bits** for the symmetric algorithm (or, greater than **768 bits** for asymmetric algorithms or greater than **128 bits** for elliptic curve algorithms)
- Same rules apply to 5D002 and 5E002(if limited)

**Exports Situations
where
Encryption Items Require
License
but
Automatic License
Exception Are Available**



Note 2: *“You can take it with you.”*

- 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.

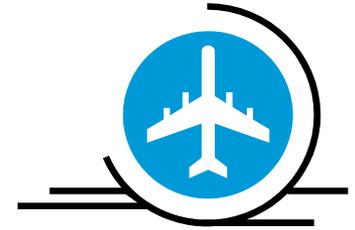
§ 740.14 – BAG – Baggage

- BAG applies to:
 - Personal effects (e.g. laptop computer with standard office use applications)
 - Household effects
 - Vehicles
 - Tools of the trade (e.g. computer with special purpose software applications)
- Note: EI commodities cannot be exported to Country Group E:1 under any circumstances or to D:1, D:2, D:3, D:4 as unaccompanied baggage



§ 740.9 – TMP

Temporary Exports



- EI products that leave the United States temporarily must be returned
 - as soon as practicable and
 - no later than a year from the date of export
- Tools of the trade – 740.9(a)(2)(i)
 - Special rules apply to Country Group E:2 and Sudan
 - Items must be under the “effective control” of the exporter or the exporter’s employee
 - Items may be shipped with the departing individual, within a month prior to departure or any time after departure

License Exception ENC § 740.17(a)

- No company registration, no self-classification/CCATS, no sales reporting
- Applies to 5A002, 5B002, 5D002, and 5E002
- **§740.17(a)(1) Internal “development” or “production” of new products**
 - “private sector end-users” HQed in Supp. 3 country
 - End use limited to internal use for the development or production of new products.
- **§740.17(a)(2) “U.S. Subsidiaries”**
 - Only to U.S. Subsidiaries as defined in 772. HQed in U.S.
 - Internal use
 - Employees of U.S. companies or U.S. subsidiaries



Lets Summarize!

No Registration or Classification Required

- Not subject - Certain publicly available object code
- EAR99 (NLR) - Medical and Note 4
- 5x992 items (NLR)
 - Related Control Note exemptions
 - Low strength encryption (≤ 56 (64)/512/112)
 - Authentication only including digital signature
- License Exceptions (TMP *, BAG, GOV, LVS, RPL, TSU*) and
 - ENC (a)(1) and (a)(2) (coming up next)

Products Designed to Use Encryption authorized under licenses, registration and classification, registration and self-classification and items exempt from encryption registration, classification and reporting requirements

Bag #	ECCNS	Authorization Required	Authorization code	Reporting	Item types:
7	5x002	Individual License or Encryption Licensing Arrangement (ELA)	License#	Semi-Annual may be required as license condition	B2
6	5x002 5x992	Registration and Classification	CCATS # (ENC/NLR)	Semi-Annual/ None	ENC B2; ENC B3 Mass Market B3
5	5x002 5x992	Registration and Self-Classification	ENC/NLR	B1	ENC B1; Mass Market B1
4	5x002	Automatic License Exception	ENC; TMP; BAG; TSU; GOV; RPL	None (except TSU)	ENC A1,A2,B4i; export meets License Exception
3	5x992	Self-Classification	NLR	None	AUTHENTICATION ONLY; LOW-STRENGTH; Related control notes; Mass Market B4i
2	EAR99	Self-Classification	NLR	None	NOTE 4 Medical Devices
1	Not Subject	Self-Classification	None	None	Certain Publicly Available Binary

Encryption Items requiring registration, classification or self-classification and reporting



License Exception ENC



License Exception ENC Part 1- CCATS Required



§ 740.17 License Exception ENC

Company Registration	CCATS	Sales Reporting	Paragraph 740.17	End User Authorization (outside E-1)	Item Description or Purpose of Export
Yes	Yes	Yes	(b)(2)	license required for Gov't end users not in Supp 3**; LE ENC for non-gov't end users***	(b)(2) commodity list
Yes	Yes	Yes for iii items only	(b)(3)	LE ENC to gov't and non-gov't end users	(b)(3) commodity list
Yes	No*	No	(b)(1)	LE ENC to gov't and non-gov't end users	not (b)(2) or (b)(3)
No	No	No	(b)(4)	LE ENC to gov't and non-gov't end users	short-range wireless
No	No	No	(a)(1)	Companies HQD in Supp 3	Dev/Production ****
No	No	No	(a)(2)	U.S. Subs	Any internal purpose ****

* Self-classification report required

** Supp 3 means end-users headquartered in Supp 3

*** License also required for cryptanalytic to gov't end users in Supp 3; for any end user outside Supp 3 for OCI items and for special (OCI, non-std, cryptanalytic) technology and for std (other) technology to D-1 countries.

**** All products developed are subject to the EAR.

§ 740.17(b)(2) ENC “Restricted”

CCATS required with 30 day wait

- Applies to 5A002, 5D002 and 5E002
- Products authorized under (b)(2) include:
 - network infrastructure products
 - certain specialized commodities and software
 - source code that is not “publicly available”
 - technology
- “**Restricted**” to non-government end-users **only**, and require a license if going to government end-users not in a Supp 3 country.
- Supp. 6 to Part 742 of the EAR required



§ 740.17 (b)(2) Criteria

(A) Network infrastructure products:

- (1) Switching equipment with throughput
> 90 Mbps;
- (2) Transmission (cable) equipment or VPN
single-channel input data rate **> 154 Mbps;**
- (3) Satellite transmission at data rates **> 10 Mbps;**
- (4) Encrypted VOIP phone systems:
 - **> 250 concurrent encrypted data channels, or**
 - **> 1,000 endpoints**

§ 740.17 (b)(2) Criteria continued

(A) Network infrastructure products: (continued)

- (5) Air-interface coverage > **1,000 meters**, and
 - (i) Max data rates > **10 Mbps** (at ranges > **1,000 meters**);
 - (ii) Maximum number of concurrent full-duplex voice channels > **30**; or
 - (iii) Substantial support is required for installation or use;

- (B) Encryption **source code** that would not be eligible for export or reexport under License Exception TSU because it is not publicly available as that term is used in §740.13(e)(1);

§ 740.17 (b)(2) Criteria continued

(C) Encryption commodities having any of the following:

(1) Been designed, modified, adapted or customized for **“government end-user(s)”**;

(2) Cryptographic functionality that has been modified or customized to **customer specification**; or

(3) Cryptographic functionality or “encryption component” (except encryption software that would be considered publicly available, as that term is used in §740.13(e)(1) of the EAR) that **is user-accessible** and can be easily changed by the user;

§ 740.17 (b)(2) Criteria continued

- (D) Encryption commodities and software that provide functions necessary for **quantum cryptography**, as defined in ECCN 5A002 of the Commerce Control List;

- (E) Encryption commodities and software that have been modified or **customized for computers** classified under ECCN 4A003;

§ 740.17 (b)(2) Criteria continued

- (F) Encryption commodities and software that provide **penetration capabilities** that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks;
- (G) **Public safety/first responder radio** (e.g., implementing Terrestrial Trunked Radio (TETRA) and/or Association of Public-Safety Communications Officials International (APCO) Project 25 (P25) standards);

§ 740.17 (b)(2) Criteria continued

(ii) Cryptanalytic commodities and software.

- LE ENC to non-“government end-users” located or headquartered in countries not listed in Supplement No. 3 to part 740 **ONLY**;

(iii) “Open cryptographic interface” items.

- LE ENC to end-user located or headquartered in a country listed in Supplement No. 3 **ONLY**.

§ 740.17 (b)(2) Criteria continued

(iv) Specific encryption technology. Specific encryption technology as follows:

- (A) Technology for “non-standard cryptography.”
 - LE ENC to end-user located or headquartered in a country listed in Supplement No. 3 **ONLY**.
- (B) Other technology.
 - NO “cryptanalytic items,” “non-standard cryptography” or any “open cryptographic interface,”
 - LE ENC to non-“government end-user” located in a country not listed in Country Group D:1 or E:1 of Supplement No. 1 **ONLY**.

§ 740.17(b)(3) ENC “Unrestricted”

Review required with 30 day wait

- A second tier of items designed to use encryption (5A002, 5B002, 5D002)
- If not B2 then review B3
- “**Unrestricted**” and may be exported to both non-government **AND** government end-users without a license.



§ 740.17(b)(3)(i)

- Specified components:
 - Chips, Chipsets, electronic assemblies, etc.
 - Cryptographic libraries, modules, development kits and toolkits
 - ASIC development kits implementing cryptography

§ 740.17(b)(3)(ii)

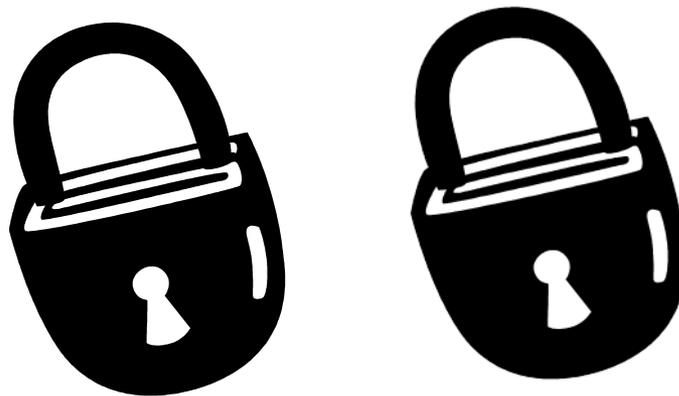
- Commodities, software and components with “non-standard encryption’.
- Non-standard cryptography means any implementation of “cryptography” involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, and GSMA) and have not otherwise been published.
- **WLAN Authentication and Privacy Infrastructure (WAPI)**

§ 740.17(b)(3)(iii)

- Computer forensic and network forensic
 - Vulnerability analysis
 - Defensive analysis
- More aggressive network penetration items are in B2
- Require semi-annual sales reporting

License Exception ENC

Part 2 – No CCATS



§ 740.17(b)(1) ENC “Unrestricted”

- Company registration required.
- CCATS NOT required
- Supplement 8 reporting required
- Self-classification (determining that item is not described by either Section 740.17(b)(2) or(b)(3)
- If not B2 and not B3 then B1
- “**Unrestricted**” and may be exported to both non-government **AND** government end-users without a license.



Lets Summarize!



§ 740.17 License Exception ENC

Company Registration	CCATS	Sales Reporting	Paragraph 740.17	End User Authorization (outside E-1)	Item Description or Purpose of Export
Yes	Yes	Yes	(b)(2)	license required for Gov't end users not in Supp 3**; LE ENC for non-gov't end users***	(b)(2) commodity list
Yes	Yes	Yes for iii items only	(b)(3)	LE ENC to gov't and non-gov't end users	(b)(3) commodity list
Yes	No*	No	(b)(1)	LE ENC to gov't and non-gov't end users	not (b)(2) or (b)(3)
No	No	No	(b)(4)	LE ENC to gov't and non-gov't end users	short-range wireless
No	No	No	(a)(1)	Companies HQD in Supp 3	Dev/Production ****
No	No	No	(a)(2)	U.S. Subs	Any internal purpose ****

* Self-classification report required

** Supp 3 means end-users headquartered in Supp 3

***License also required for cryptanalytic to gov't end users in Supp 3; for any end user outside Supp 3 for OCI items and for Special (OCI, non-std, cryptanalytic) technology); and for std (other) technology to D-1 countries.

****All products developed are subject to the EAR.



Mass Market Encryption



What is Mass Market?

- Hardware and software described by the Cryptography Note
 - (Note 3 to Category 5 part II, Information Security)
 - Origins in the General Software Note -GSN
 - Items so widely distributed that export control is not realistic and certain components of those items
- Cryptography Note is GSN for encryption
- Decontrolled from 5X002 to 5X992

Examples of “Mass Market” Products

- Mass market b1 products
 - General purpose operating systems
 - Short range wireless devices such as access points
 - PDAs and Cell Phones including smartphones
 - Commercial off the shelf (“COTS”) software for personal computers
 - Home and small office networking commodities
- Mass market b3 products
 - Chips (MM B3 if mass marketed themselves)
 - Toolkits



Cryptography Note

Note 3 to Category 5 – Part 2

ECCNs 5A002 and 5D002 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 be easily 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 described in paragraphs (a) through (c) of this note.

Lower and higher strength mass marketed products

- Lower strength mass marketed products may be self-classified as 5x992
 - key lengths not exceeding 64 symmetric; 768 asymmetric; or 112 elliptic curve
 - no registration or Supplement 8 reporting required
- Higher strength mass market products are initially 5x992 but become 5x992 after classification or self-classification
 - require registration
 - Require Supplement 8 reporting
- Higher strength mass market products may require classification

Which mass marketed products can be self-classified?

- Mass marketed products described by 742.15(b)(2) are not eligible for mass market treatment
- Mass Market products in 742.15(b)(3) require BIS classification and cannot be self-classified
 - Chips, chipsets, etc.
 - “non-standard” cryptography
 - Cryptographic libraries, modules and development kits
 - Application-specific development kits implementing cryptography
 - Enabling items
- Others can be self-classified under 742.15(b)(1) with Supplement 8

OVERVIEW OF CHANGES TO MASS MARKET (MM) CRYPTOGRAPHY NOTE

Note 3 to CAT 5 Part 2 is changed in 3 ways

1. Previous text is renumbered as Paragraph a.
2. A new Paragraph b decontrols to ECCN 5A992 certain components not separately sold to the public via retail channels except as part of MM products
3. New Note to Cryptography Note added to help industry better understand existing MM provisions and requirements related to Paragraph a.



OVERVIEW (CONT'D)

- New (renumbered Paragraph a.) still applies to components which are themselves sold in MM channels
- **CURRENT EAR REQUIREMENTS STILL APPLY TO PARA A AND B:**
 - B2 Products/Components are NOT eligible for MM treatment.
 - Classification request required for all 742.15(B)(3) components (Para A and Para B) except as specifically grandfathered
 - Supplement 8 reporting rules apply to 742.15(b)(1) items for both paragraphs



SCOPE OF NEW PARA B

- Hardware components not mass marketed (e.g. OEM only) if
 - components of an existing mass market (MM) items
 - factory-installed into a Paragraph “A” MM product, and
 - functionally equivalent aftermarket replacements
 - identical in form, fit and function to OEM components
- Paragraph b. text only mentions hardware components
 - also applies to certain software components
 - If specially designed for a particular hardware component that has already been released from control.



PARA B COMPONENTS REQUIREMENTS



- End-product must first be established as MM
- Primary function(s) **NOT** “information security.”
- Cannot introduce new cryptographic functionality or enhance existing cryptographic functionality of MM products
- Cannot transform product to a non-consumer type item
- Cannot provide custom/substitute cryptography (even if same algorithm)

GRANDFATHERING

- If a Paragraph b. component has been previously been classified under ECCN 5A002 pursuant to §740.17(b)(3) or §740.17(b)(1):
 - a new classification by BIS is NOT required
 - may be self-classified as §742.15(b)(3) or §742.15(b)(1) but must be included as such in a self-classification report submitted to BIS in January 2014

Note: Grandfathering language in 740.17(d)(2) does not make clear that previous 740.17(b)(1) products that are also Para. b components would be self-classified under §742.15(b)(1), not (b)(3).



CLASSIFICATION AND SELF-CLASSIFICATION OF NEW ITEMS UNDER PARA B



- Procedure for Paragraph (b) classification of new products or products not grandfathered:
 - Components described by § 742.15(b)(3) must be submitted to BIS for classification as 5A992.
 - Components described by Paragraph (b) but not described as components by § 742.15(b)(3)
 - May now be self-classified as 5A992 under §742.15(b)(1).
 - Examples of items that might be Paragraph (b) components but not described in 742.15 (b)(3): stand-alone disk drives, network adapter cards, and computer boards (essentially a computer without a shell) marketed only to OEMs.
 - All 742.15(b)(1) items classified under Paragraph (b) must be included in the Annual Supplement 8 self-classification report



New Note to the Cryptography Note Clarifies How to Classify MM

- Paragraph 1 provides specific guidance of what it means to be ‘mass market’ and ‘generally available to the public’ under Para. a .
- The new Note to the Cryptography Note does not change the scope of mass market controls
- Illuminates past and current practices by BIS in classifying mass market items



New Note to Crypto Note (cont'd)

- To be described by Para. a, the item must meet all of the following
 - must be of potential interest to a wide range of individuals and businesses
 - potential customers are not dependent on the supplier to learn how much the item costs or its main functional specifications. The manufacturer must provide such information to the general public.
- Relevant factors such as quantity, price, technical skill, existing sales channels, typical customers, typical use, or any exclusionary practices of the supplier may be taken into account in determining whether Para. A conditions are met.



BIS Review of Mass Market Classifications

- Applicant Must show **how** product meets the “Cryptography Note” criteria
- Must provide Marketing information--generally available to the public
 - Who buys it, why and how is it marketed
 - Ballpark pricing and number of sales to different user
 - Why the general public would use it
 - Screen shots of mass market sales are useful
 - Discuss how product is installed and used without support
- Technical information--Show that the B2 criteria do not apply
 - Items described in 740.17(b)(2) are not mass market
 - Provide Brochures / tech specs
 - Required Supp 6 encryption technical information
 - State no source code (source code is easily user modifiable)

MASS MARKET “B1” ITEMS CAN BE EXPORTED IMMEDIATELY IF THEY ARE

- **MASS MARKET COMMODITIES AND SOFTWARE THAT WERE**
 - CLASSIFIED BY BIS PRIOR TO JUNE 2010 AND GRANDFATHERED OR
 - SELF-CLASSIFIED BY THE MANUFACTURER (OR YOU) AS 742.15(b)(1)
 - Not described by 740.17(b)(2) and
 - Not described by 740.17(b)(3) and
 - Not described by 742.15(b)(3)

and

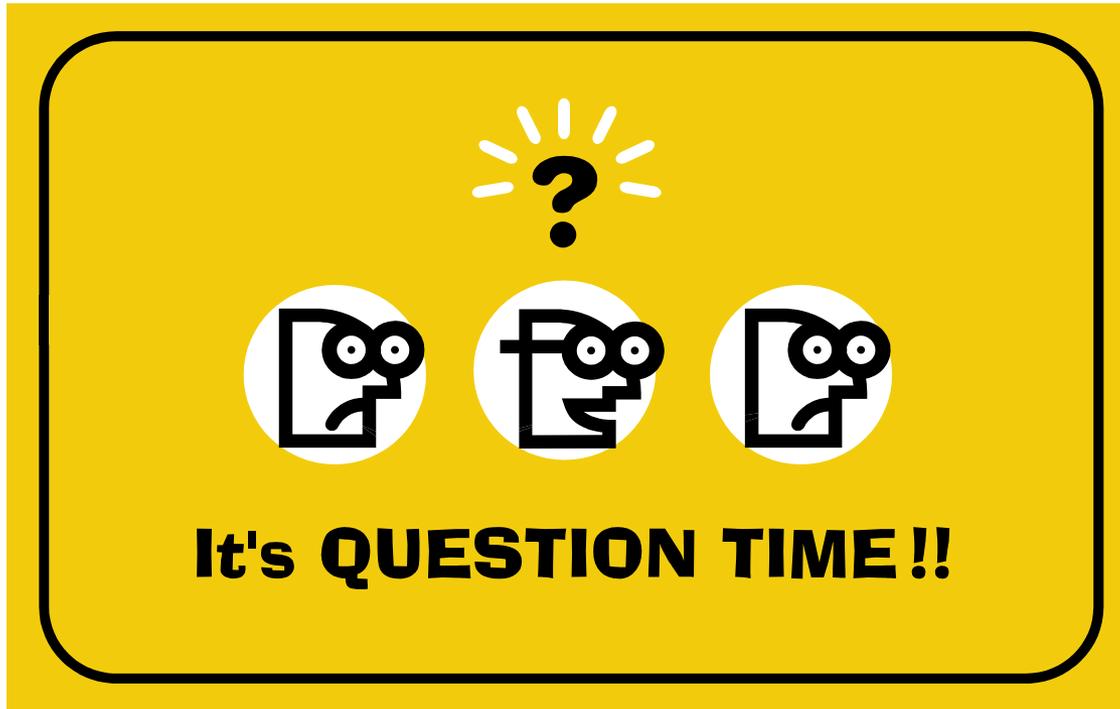
- YOU OR THE MANUFACTURER HAS OBTAINED AN ERN (ENCRYPTION REGISTRATION NUMBER)

and

YOU OR THE MANUFACTURE WILL FILE A SUPPLEMENT 8 REPORT

MASS MARKET “B3” ITEMS CAN BE EXPORTED AS FOLLOWS

- **Immediately** if they were classified by BIS prior to June 2020 and grandfathered
- OR
- **Immediately** after registration and submission of a classification request
 - To ‘Supplement 3’ countries
 - To foreign subsidiaries of Canadian & ‘Supplement 3’ country companies
 - **30 days after** submission of a classification request
 - Outside ‘Supplement 3’ countries
 - Unless notified by BIS that review request held without action (HWA) for more information
 - -- 30 days excludes time on HWA
- and*
- THE PARTY SUBMITTING THE CLASSIFICATION REQUEST (YOU OR THE MANUFACTURER) HAS AN ERN (ENCRYPTION REGISTRATION NUMBER)



Information Technology Controls Division

Randy Wheeler

Director

Ph: 202-482- 5303

E-mail:

catherine.wheeler@bis.doc.gov

Judith Currie

Senior Export Policy Analyst

Ph: 202-482-5085

E-mail: judith.currie@bis.doc.gov

Sylvia Jimmison

Export Policy Analyst

Ph: 202-482-2342

E-mail: sylvia.jimmison@bis.doc.gov

Anita Zinzuvadia

Electrical Engineer

Ph: 202-482-3772

E-mail: anita.zinzuva@bis.doc.gov

Michael Pender

Senior Engineer

Ph: 202-482-2458

E-mail: michael.pender@bis.doc.gov

Aaron Amundson

Export Policy Analyst

Ph: 202-482-5299

E-mail: aaron.amundson@bis.doc.gov

Products Designed to Use Encryption authorized under licenses, registration and classification, registration and self-classification and items exempt from encryption registration, classification and reporting requirements

Bag #	ECCNS	Authorization Required	Authorization code	Reporting	Item types:
7	5x002	Individual License or Encryption Licensing Arrangement (ELA)	License#	Semi-Annual may be required as license condition	B2
6	5x002 5x992	Registration and Classification	CCATS # (ENC/NLR)	Semi-Annual/ None	ENC B2; ENC B3 Mass Market B3
5	5x002 5x992	Registration and Self-Classification	ENC/NLR	B1	ENC B1; Mass Market B1
4	5x002	Self-Classification and License	ENC; TMP; BAG; TSU; GOV; RPL	None (except TSU)	ENC A1; ENC A2 ; ENC B4i; export meets License Exception conditions
3	5x992	Self-Classification	NLR	None	AUTHENTICATION ONLY; LOW-STRENGTH ; Related control notes; Mass Market B4i
2	EAR99	Self-Classification	NLR	None	NOTE 4 Medical Devices
1	Not Subject	Self-Classification	None	None	Publicly Available Binary where either source is TSU or free mass marketed binary that has is initially self-classified and reported per bag 5