Encryption Workshop

Update 2013

U.S. Department of Commerce
Bureau of Industry and Security

Encryption

- Wassenaar 2012 amendments
  - Mass Market Note
    - Components
    - Note
  - Other Category 5, part 2 amendments
  - Interception (ECCN 5A001)
- Classification and registration issues
- Encryption Licensing Arrangements

U.S. Department of Commerce
Bureau of Industry and Security

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

JUNE 20, 2013 WASSENAAR AMENDMENTS TO THE CRYPTOGRAPHY NOTE (MASS MARKET)

AND OTHER AMENDMENTS TO ENCRYPTION EXPORT CONTROLS

U.S. Department of Commerce
Bureau of Industry and Security

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

OVERVIEW OF CHANGES TO MASS MARKET (MM) CRYPTOGRAPHY NOTE

1. Previous text renumbered as Paragraph a.
2. A new Paragraph b. decontrols certain components of MM products
3. New Note to Cryptography Note explains mass market criteria listed under Paragraph a.

U.S. Department of Commerce
Bureau of Industry and Security

OVERVIEW (CONT'D)

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Paragraph a. still applies to components which are themselves sold in MM channels
- **EAR requirements apply to both Paragraphs 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 b.) except as specifically grandfathered
  - Supplement 8 reporting rules apply to 742.15(b)(1) items for both paragraphs

U.S. Department of Commerce
Bureau of Industry and Security

Scope of New Paragraph b.

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Hardware components not mass marketed (e.g. OEM only) if
  - components of an existing MM item
  - factory-installed into a Paragraph a. MM product
  - functionally equivalent aftermarket replacements are 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.

U.S. Department of Commerce
Bureau of Industry and Security

Paragraph b. Requirements

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- End-product must first be established as MM
- Primary function(s) **NOT** ‘‘information security.’’
- Cannot introduce new 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)

U.S. Department of Commerce
Bureau of Industry and Security

Grandfathering

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- If a Paragraph b. component has been previously 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: Previous 740.17(b)(1) products that are also Paragraph b. components would be self-classified under §742.15(b)(1), not (b)(3).

U.S. Department of Commerce
Bureau of Industry and Security

Classification and Self-classification of Items under Paragraph b.

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Components described by § 742.15(b)(3) must be submitted to BIS for classification as ECCN 5A992.
- Components described by Paragraph b. but not described as components by § 742.15(b)(3)
  - May now be self-classified as ECCN 5A992 under §742.15(b)(1).
  - Examples: 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

U.S. Department of Commerce
Bureau of Industry and Security

New Clarification Note to the Cryptography Note

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Paragraph 1: guidance on 'mass market' and 'generally available to the public' under Paragraph a.
- Paragraph 2: factors to be considered
- The new Note to the Cryptography Note does not change the MM criteria

U.S. Department of Commerce
Bureau of Industry and Security

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

OTHER JUNE 20, 2013 WASSENAAR CHANGES AS THEY RELATE TO ENCRYPTION EXPORT CONTROLS

- **New paragraph 1 – "specially designed"**
- **Parameter changes for PAN Note I**
- **Copy-protected excluded from both 5x002 and 5x992**
- **Cryptanalysis by reverse engineering**
- **5E002 includes technical data obtained by evaluation**

U.S. Department of Commerce
Bureau of Industry and Security

Changes to ECCN 5A001

Effective June 20, 2013

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

Before the rule change		After the rule change
• 5A001.i	→	• 5A001.f1
• 5A001.f1	→	• 5A001.f2
• 5A001.f2	→	• 5A001.f3
		• New 5A001.f4

U.S. Department of Commerce
Bureau of Industry and Security

ECCN 5A001 as of June 2013

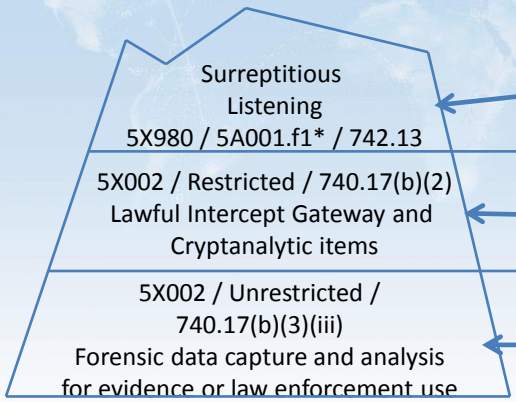
Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- 5A001.f1 – Interception equipment designed for the extraction of voice or data, transmitted over the air interface;
- 5A001.f2 – Interception equipment not specified in 5A001.f.1, designed for the extraction of client device or subscriber identifiers (e.g. IMSI, TIMSI or IMEI), signaling, or other metadata transmitted over the air interface;
- 5A002.f3, f.3.a, f.3.b, f.3.c: Jamming equipment …
- 5A001.f4 – Radio Frequency (RF) monitoring equipment designed or modified to identify the operation of items specified in 5A001.f.1, 5A001.f.2 or 5A001.f.3

U.S. Department of Commerce
Bureau of Industry and Security

Communications Intercepting Devices

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy



Licenses are required for all end users and all destinations **Not eligible for LE ENC**

Eligible for LE ENC after registration and classification.

Eligible for LE ENC after registration and classification

*SL includes 5A001.f1; 5D001 for equipment, functions, features, or characteristics controlled by 5A001.f1; 5E001 for the "development" or "production" of equipment, functions or features controlled by 5A001.f1 or the "development" or "production" of software controlled by 5D001.a for 5A001.f1.

U.S. Department of Commerce
Bureau of Industry and Security

Is my item subject to the 742.13 Communications Interception policy?

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

1. Does your item intercept or facilitate the intercept of wire, speech or electronic communications?

2. Does your item implement any of the FCC, ETSI, 3GPP or ATIS standards for lawful intercept?

3. Is the item specially designed or limited to use only on private network addresses?

U.S. Department of Commerce
Bureau of Industry and Security

Is my item subject to the 742.13 Communications Interception policy?

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- 4. Is there a warning to the user that their communications may be monitored or recorded?

- 5. Besides monitoring communications, what are other purposes for which the item is marketed and used?

U.S. Department of Commerce
Bureau of Industry and Security

Classification Issues

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Section 740.17(b)(2) versus mass market
- Classifications of components versus products
- Development kits under 740.17(b)(3) and 742.15(b)(3)
- Encryption Registrations

U.S. Department of Commerce
Bureau of Industry and Security

Section 740.17(b)(2) v. Mass Market

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

Section 742.15(b): “Encryption items that are described in §§ 740.17(b)(2) or (b)(3)(iii) of the EAR do not qualify for mass market treatment.”

U.S. Department of Commerce
Bureau of Industry and Security

Components Versus Products

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

The classification of an encryption component does not necessarily determine the classification of the product that uses the component.

U.S. Department of Commerce
Bureau of Industry and Security

Development Kits Under 740.17(b)(3) and 742.15(b)(3)

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

(i) Specified components . . . as follows:

. . .

(B) Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);

(C) Application-specific hardware or software development kits implementing cryptography.

U.S. Department of Commerce
Bureau of Industry and Security

Encryption Registrations

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Various system limitations
- Updating or cancelling a company registration

U.S. Department of Commerce
Bureau of Industry and Security

Encryption Licensing Arrangements

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

U.S. Department of Commerce
Bureau of Industry and Security

ELAs

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Broad authorization for exports not eligible for License Exception ENC (most (b)(2) items to government end users in countries not listed in Supplement No. 3 to part 740)
- "Less sensitive" government end users –
  - "worldwide ELA" – 4-year validity – semi-annual sales reporting
- "More sensitive" government end users –
  - "single country ELAs – 4-year validity –
  - 15-day pre-shipment notification

U.S. Department of Commerce
Bureau of Industry and Security

ELAs

Export Control Reform: Fulfilling the Promise
UPDATE
Conference on Export Controls and Policy

- Letter authorization to add new products to existing ELAs after issuance of CCATS
  - New product lines
  - New versions of previously-approved products

U.S. Department of Commerce
Bureau of Industry and Security