Encryption Simplification and the October 3rd rule

Michael Pender

Senior Engineer

Information Technology
Controls Division

Agenda

- Introduction
- Overview of the Encryption Simplification Process and the October 3rd Rule
- Summary of changes
- New structure for License Exception ENC:
  - No review required, no reporting
  - No review required, with reporting
  - Review Required, no waiting
  - Review Required, with waiting period
- Questions and Answers

Introduction

Overview of Encryption Simplification and the October 3rd Rule

Summary of Changes

- License Exception (LE) ENC restructured based on the type of review and the waiting period
- Removed Section 744.9 and revised ECCN 5E002 to clarify current control list restrictions pertaining to technical assistance by U.S. persons
- Removed notification requirements for items classified as 5A992, 5D992 and 5E992
- Removed LE KMI as obsolete

Summary of Changes (cont'd)

- Bulgaria, Canada, Iceland, Romania and Turkey were added to the list of countries that receive favorable treatment under LE ENC (Supplement 3 to Part 740)
- Excludes certain items from review and/or reporting requirements including "personal area network" commodities and "ancillary cryptography" items
- Revised "Guidelines for Submitting Review Requests for Encryption Items"

Summary of Changes (cont'd)

- Makes it clear that commodities and software pending mass market review are authorized by LE ENC under ECCNS 5A002 and 5D002. After the mass market review is complete, such commodities and software may be exported under ECCNs 5A992 and 5D992 using No License Required (NLR)
- Increases certain parameters under License Exception ENC Restricted.

No Review Required, No Reporting

- Exports to "Private sector end users" in countries in Supplement 3 to Part 740 (§740.17(a)(1)) (for internal development or production of new products, only)
- To U.S. subsidiaries (§ 740.17(a)(2)) and employees of U.S companies (internal use)

No Review Required, No Reporting: Short Range Wireless Items

- Short-range wireless items not controlled under Cat. 5 (§§ 740.17(b)(4)(i) and 742.15(b)(3)(ii))
  - Nominal range ≤100 meters
  - Examples: some* 802.11 and 802.15.1
- May self classify under 5x002 or 5x992 as appropriate.

No Review Required, No Reporting: Wireless PAN

"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).

- ≤ 30 meters
- 802.15.1: class 2 and 3, but not class 1
- May Self Classify as 5x002 or 5x992, as appropriate

Bluetooth™

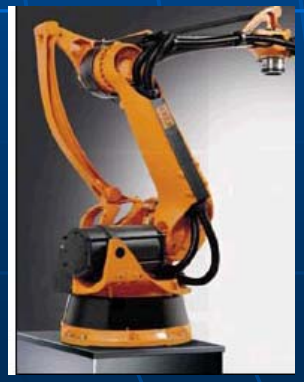
No Review Required, No Reporting Wireless PAN Examples

- Hands-free headsets
- Wireless networking between personal computers
- Wireless mice, keyboards, printers
- GPS receivers with Bluetooth interfaces*
- Bar code scanners
- Wireless controllers for game consoles
- Software for transfer of files using OBEX

No Review Required, No Reporting "Ancillary Cryptography"

"Ancillary Cryptography" 740.17(b)(4)(iv): not primarily useful for computing (including the operation of "digital computers"), communications, networking (includes operation, administration, management and provisioning) or "information security".

- **May Self Classify as 5x002 or 5x992, as appropriate**



No Review Required, No Reporting "Ancillary Cryptography" Examples

- Piracy and theft prevention for software, music, etc.
- Games and gaming
- Household utilities and appliances
- Printing, reproduction, imaging and video recording or playback
- Business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery)
- Industrial, manufacturing or mechanical systems (e.g., robotics, heavy equipment, facilities systems such as fire alarm, HVAC)
- Automotive, aviation, and other transportation systems

Mass Marketed Products
No Review Required

- Short-range wireless encryption functions (742.15 (b)(3)(i))
- Wireless "personal area network" items (742.15 (b)(3)(ii))
- "Ancillary cryptography" (742.15 (b)(3)(iii))

740.17 License Exception ENC- Encryption

Paragraph 740.17	End User authorized (Outside E-1)	Item Description or Purpose of Export	Review Required?
(a)(1)	Private in Supp 3	Dev/Production only	No Review*
(a)(2)	U.S. Subs	Any internal purpose	No Review*
(b)(1)(i)	In Supp 3	End Use or Transfer	Review no waiting
(b)(1)(ii)	Outside Supp 3	≤80/1024/160 and Source code	Review no waiting
(b)(2)	No Gov't outside Supp 3	Any purpose	Review with 30 day wait
(b)(3)	All except E-1	Any purpose	Review with 30 day wait
(b)(4)	All except E-1	Short-range Wireless Wireless PAN; Ancillary Crypto	No Review
(e) Reporting required for (b)(1), (b)(2), and (b)(3), (b)(4)(ii)			

*All products developed are subject to the EAR and require review

No Review Required, No Reporting: Section 740.17(a)

- Applies to 5A002, 5B002, 5D002, and 5E002

- **§740.17(a)(1) Internal "development" or "production" of new products**
  - No review, notification or reporting
  - Only to "private sector companies" 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**
  - No review, notification or reporting
  - Only to U.S. Subsidiaries as defined in 772. HQed in U.S.
  - Internal use
  - Employees of U.S. companies or U.S. subsidiaries

Review Required, no Waiting Period: Section 740.17(b)(1)

- Applies to 5A002, 5B002, and 5D002

- **§740.17(b)(1)(i) Review required without waiting period to Supp 3 Countries**
  - Review Required prior to export
  - Can export *immediately* after **complete** submission
  - Only to Supplement 3 private companies and governments
  - End use is not limited
  - *pending* mass market reviews may be exported under this sec.
  - Also includes 5E002

- **§740.17(b)(1)(ii) Review required without waiting period to Non-Supp 3 Countries**
  - ≤80 bits Symmetric
  - ≤1024 bits Asymmetric
  - ≤160 bits Elliptic Curve
  - Source Code to non-government end users

Review Required, with Waiting Period: § 740.17(b)(2) ENC "Restricted"

- Applies to 5A002, 5B002, and 5D002
- Products authorized under (b)(2) include:
  - network infrastructure products
  - source code that is not "publicly available"
  - certain specialized commodities and software
- Require a license if going to government end-users not in a Supp 3 country.
- Question 11 of Supp. 6 means "evaluate your products against B2 Criteria"

§ 740.17 (b)(2)(i)-(vi) Criteria

(i) **Network infrastructure** items with any of the following:

(A) Aggregate encrypted WAN, MAN, VPN or backhaul throughput exceeding **90** Mbps.; or

(B) Single-channel input data rate **exceeding 154 Mbps**; or

(C) **250 concurrent encrypted data channels, or encrypted signaling to more than 1,000 endpoints for VOIP or converged products**; or

(D) Air-interface coverage exceeding 1,000 meters, with:
(1) Maximum data rates >**10** Mbps (at >1,000 meters); or
(2) Max # of concurrent full-duplex voice channels >30; or
(3) Substantial support is required for installation or use.

§ 740.17 (b)(2)(i)-(vi) Criteria
cont.

(ii) Encryption source code not authorized by EAR §740.13(e)(1)

(iii) Encryption items:

(A) that have been modified or customized for government end-user/ end-use (e.g., **(SOC/NOC);** or

(B) modified or customized to customer specifications; or

(C) user-accessible & easily changed by user.

(iv) "Cryptanalytic items"; or

(v) Providing functions necessary for quantum cryptography; or

(vi) Modified for computers controlled by ECCN 4A003

Review Required, with Waiting Period: § 740.17(b)(3) ENC "Unrestricted"

- Everything else designed to use encryption (5A002, 5B002, 5D002)
- If not B2 then B3
- If not Mass Market then B3.
- Export to both non-government **AND** government end-users without a license.

No Review Required, No Reporting: 740.17 (b)(4)

- Short-range wireless encryption functions
- Foreign products developed with US-origin encryption source code, components or toolkits
- Wireless “personal area network” items
- “Ancillary cryptography”

Modifications to a Reviewed Product

- New review needed:
  - Changes Cryptographic functionality affecting License Exception ENC eligibility
- New review NOT needed:
  - Modifications do not change cryptographic functionality
    - Name changes, version changes, updates to 3rd party encryption library
- See "Note to paragraph (b)" at end of 740.17(b)

Guidance on the Web

Step by step guidance to exporters for preparing review requests and notifications:

http://www.bis.doc.gov/encryption

- EAR on the web:
  - www.access.gpo.gov/bis/ear_data.html
- Specific questions:
  - Information Technology Controls Division
    - ENCRYPTION HOTLINE: (202) 482-0707

Information Technology Contacts

Randy Pratt
Director
Ph: 202-482- 5303
E-mail: cpratt@bis.doc.gov

Michael Pender
Senior Engineer
Ph: 202-482-2458
E-mail: mpender@bis.doc.gov

Joe Young
Senior Engineer
Ph: 202-482-4197
E-mail: jyoung@bis.doc.gov

Judith Currie
Senior Export Policy Analyst
Ph: 202-482-5085
E-mail: jcurrie@bis.doc.gov

Sylvia Jimmison
Export Policy Analyst
Ph: 202-482-2342
E-mail: sjimmiso@bis.doc.gov

Aaron Amundson
Export Policy Analyst
Ph: 202-482-5299
E-mail: aamundso@bis.doc.gov

Anita Zinzuvadia
BIS-Western Regional Office
Electrical Engineer
Ph: 949-660-0144x131
E-mail: azinzuva@bis.doc.gov