Encryption Controls

Moderator: Joseph Young
Acting Director
Information Technology Controls
Division



Encryption Controls - Update 2012

Information Technology Controls
Division
July 19, 2012



Agenda

- Recent ITCD activities
- Presentations
 - 1. Jan. 7, 2011 Rule Mike
 - 2. Note 4 Anita
 - 3. Encryption Submission Requirements Judy
 - 4. Encryption technology controls Aaron
- Roundtable discussions and Q's and A's



7/19/2012

Information Technology Controls Division (ITCD)

- Category 4: Computers
- Category 5, Part 1: Telecommunications
- Category 5, Part 2: Information Security
 - –Encryption
 - Others
- Now include deemed exports



Category 4: Computers

- 4A003.b
- from 1.5 to 3.0 WT
- Deemed exports
 - Computer Tier 1 countries (740.7(c)(3))
 - From 1.5 to 25 WT for "development" and "production" technologies
 - From 3 to 120 WT for "use" technologies
 - Computer Tier 3 countries (740.7(d)(3))
 - From 0.5 to 12 WT for "development" and "production" technologies
 - From 0.75 to 25 WT for "use" technologies



Category 5, Part 1: Telecommunications WA 11 agreements

- 5A001.i mobile intercept equipment
 - New entry.
 - Covered under 5A980 for SL reason
 - No License Exception per §740.2 (a)(3)
- 5E001.c technology for digital transmissions
 - "development" and "production" technology from50 to 120 Gbit/s

Category 5, Part 2: WA Info-Sec Proposal

- Amending Note 3 (Cryptography Note) to make it available for components for use in the production of mass-market products
- No agreement in WA 11
- U.S. has resubmitted this proposal for discussion



1. Encryption Software Not Subject to the EAR

76 FR 1059 (AKA the January 7, 2011 rule)



Encryption Software Not Subject to the EAR

I. "Publicly available" mass market encryption object code software

Note: if the symmetric key length is greater than 64-bits, then registration and classification are still required

II. "Publicly available" encryption software that is classified under ECCN 5D992 for reasons other than a "mass market" determination

III. "Publicly available" encryption object code classified under ECCN 5D002 on the Commerce Control List when the corresponding source code meets the criteria specified under License Exception TSU

7/19/2012

Example 1

- Cryptographic software specially designed for banking or money transaction use as described by Note d to ECCN 5A002
 - The item is eligible for self-classification
 - Registration is NOT required
 - Filing a self-classification report is NOT required
 - If the exporter makes the software "publicly available," then it is not subject to the EAR



Example 2

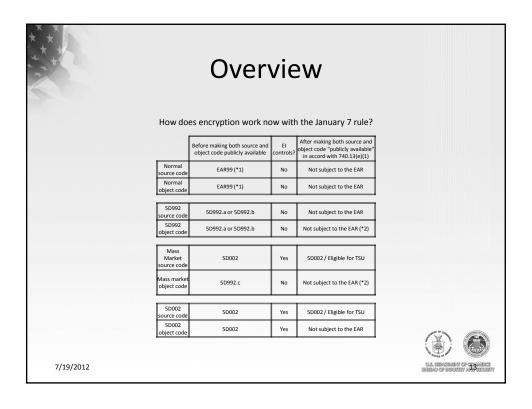
- A communications application for smart phones that uses AES-128 is mass marketed
 - Registration is required
 - The app is eligible for self-classification
 - Filing a self-classification report is required
 - If the application did not use strong cryptography (AES-128) then neither registration nor selfclassification is required
 - If the exporter makes the software "publicly available," then it is not subject to the EAR

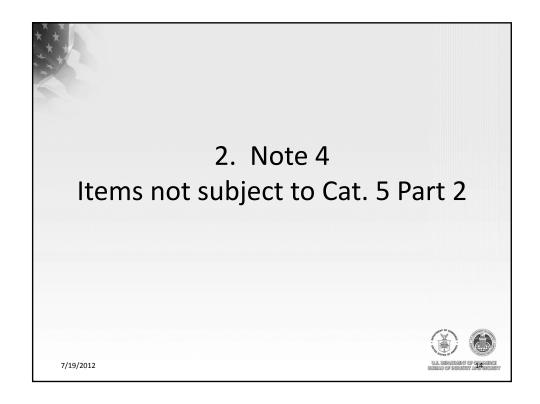
7/19/2012

Example 3

- Operating system software object code when BOTH the object code and corresponding source code are "publicly available" and eligible for TSU
 - Notification must be provided in accord with 740.13(e)(1)
 - Previously, the object code was eligible for export under TSU, but it was still subject to the EAR
 - Now the object code is released from contro







Not encryption Note 4 to Cat 5 Part 2

- The primary function is not:
 - "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 management); or
 - Networking (includes operation, administration, management and provisioning);

AND

Encryption supports primary function



7/19/2012

Example 1

- Electronic medical record keeping software for doctors to manage patients' medical data.
 - Allows doctors to send, receive and store patients' medical diagnostic results per HIPPA. Encryption used to secure communication.



Example 2

- Television set with internet connectivity that allows users to also video chat, IM, email, listen to music, surf the internet, use video on demand, etc.
 - Encryption is used to secure communications





7/19/2012

Example 3

- Industrial controller in a dishwasher that allow the machine to be remotely serviced
 - Dishwasher vs. controller component
 - General use vs. Specific use







Submission Requirements

- Encryption Registration
- Classification
- Self-Classification
- Reporting
- Licenses



Encryption Registrations Encryption Registration Numbers (ERNs)

- Attach pdf of Supplement 5 to Part 742 information to the new Encryption Registration work item in SNAP-R
- System automatically responds with an ERN in about an hour
- ERN is required before export of items self-classified under
 - 740.17(b)(1) or
 - 742.15(b)(1)
- Encryption registration number (ERN)must be placed in Additional Information block when submitting classification requests under
 - 740.17 (b)(2) and (b)(3)
 - 742.15(b)(3)





7/19/2012

Encryption Registration (cont'd).

- Registration/reporting unit is usually a company
- Can rely on manufacturer's registration/ selfclassification and reporting
- Do not resubmit each year unless information you provided on the first registration changes - Only one registration per reporting unit per year
- Updating a company registration



CCATS Classification

- Classification by BIS/NSA Required
 - "Restricted" items under ENC 740.17(b)(2)
 - "Unrestricted" items under ENC 740.17(b)(3)
 - Listed mass market items 742.15(b)(3))
- Self-classification permitted for other items

7/19/201

Self-classification

- BIS continues to receive many requests for items eligible for self-classification
- Such classification requests are not referred to NSA
- Sufficient product information must be submitted; Supplement No. 6 is "generally" not required
- Annual Supplement 8 report required for "B1" items even if submitted for classification by BIS



Semi-annual Sales Reporting (§ 740.17(e))

- Now applies only to (B)(2) and (B)(3)(iii)
- Product name, quantity and recipient(s)
 - Distributors or other resellers
 - Direct sales
- Information on foreign products developed
- Reports to both BIS and the ENC Encryption Request Coordinator

7/19/2012

Annual Report of Exported Products ("Supplement 8 Report")

- All (B)(1) items (items self-classified under 740.17 (b)(1) and 742.15 (b)(1)
- Submitted by email to NSA and BIS
- CSV (comma separated values) format
- Six specified data fields: name of product, model number, manufacturer, ECCN, ENC or mass market, item type (of 49 listed)
- Items classified under (B)(2) or (B)(3) should not be listed (740.17 (b)(2/3) and 742.15 (b)(3)

4. Encryption Technology Controls

7/19/2012



Overview of Technology Controls in 740.17(b)(2)

The June 2010 rule differentiates among 4 types of encryption technology:

- Cryptanalytic Technology
- "Open Cryptographic Interface" Technology
- Technology for "non-standard cryptography"
- Other Technology



Tips for Reading the Technology Controls in 740.17(b)(2)

- The specific subparagraph in (b)(2) should be read in conjunction with the Note to introductory text of paragraph (b)(2).
- The word "item" means "item" as defined in Section 772.

7/19/2012



Technology Authorized under License Exception ENC

- Cryptanalytic Technology
 - Authorized to non- "government end-users" located or HQ'd in Supp. 3
 - Introductory Note 3
 - 740.17(b)(2)(ii) only for commodities and software
- "Open Cryptographic Interface" Technology
 - Authorized to any end-user located or HQ'd in Supp. 3
 - Introductory Note 1 and 4 and 740.17(b)(2)(iii)



Technology Authorized under License Exception ENC (cont.)

- Technology for "non-standard cryptography"
 - Authorized to any end-user located or HQ'd in Supp. 3
 - Introductory Note 1 and 4 and 740.17(b)(2)(iv)(A)
- -Other Technology
 - Authorized to:
 - Any end-user located or HQ'd in Supp. 3; and
 - Any non- "government end-user" located outside of Country Group D:1
 - Introductory Note 1 and 740.17(b)(2)(iv)(B)

7/19/2012

Information Technology Controls Division

Randy Pratt

Director

Ph: 202-482- 5303

E-mail: catherine.pratt@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.zinzuvadia@bis.doc.gov

Joseph Young

Acting Director and Senior Engineer

Ph: 202-482-4197

E-mail: joseph.young@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

