Morgan Lewis

EAR Encryption Regulations: A New Enigma Machine or a Mystery Wrapped in a Riddle

TECHNOLOGY MAY-RATHON

Margaret Gatti and Marynell DeVaughn

June 9, 2016

Agenda

- Evolution of EAR Encryption (EI) Controls
  - Key EI Regulatory Concepts – A Unique Control Regime
  - Commerce Control List, Supplement No. 1 to Part 744, Category 5, Part 2, "Information Security"
  - License Requirements and License Exception ENC
  - Notes 3 and 4
  - Decision Trees
  - Reporting Requirements
- Misconceptions
- Challenges/Compliance Risks
  - Acquisitions
  - Third Party Component Classification
  - Outsourced IT
  - Wassenaar Arrangement (WA) Implementation

Key Regulatory Concepts

- ERN (Encryption Registration Number)
- License Requirements
- License Exception ENC
- Self-Classification
- BIS Classification
- Note 3 – Cryptography Note ("Mass Market")
- Note 4 - "Ancillary" Encryption
- Reporting – Annual/Semi-Annual
- See-through Rule vice De Minimis
- Public Domain/Publicly Available Encryption

Relevant ECCNs and Reasons for Control

- 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

Key Provisions of License Exception ENC EAR § 740.17(a)

- 740.17(a):
  1. Authorizes exports to private sector end-users (individuals not acting on behalf of a foreign government, or commercial firms not owned by, controlled by, or acting on behalf of a foreign government) that are headquartered in a country listed in Supplement No. 3 to Part 740 for internal development or production of new products.

OR

  2. Authorizes exports to subsidiaries of U.S. companies for internal use

Key Provisions of License Exception ENC EAR § 740.17(b)(1)

- 740.17(b)(1) is a catch-all – applies to encryption items except items described in 740.17(b)(2) and (b)(3)
  - Requires encryption registration
  - Authorizes export to non-government end-users and government end-users located in all countries except embargoed/terrorist-designated countries (e.g., Crimea region of Ukraine, Cuba, Iran, North Korea, Sudan and Syria

Key Provisions of License Exception ENC EAR § 740.17(b)(2)

- Products authorized under (b)(2) include:
  - network infrastructure products
  - certain specialized commodities and software
- Requires encryption registration
- Authorizes exports to:
  - End-users in Supplement No. 3 countries;
  - Only non-government end-users outside of Supplement No. 3 countries (excluding embargoed/terrorist-designated countries)
- Does not authorize exports to:
  - Government end-users outside of Supplement No. 3 countries – a license is required

Key Provisions of License Exception ENC EAR § 740.17(b)(3)

- Key products authorized under (b)(3) include:
  - Commodities, software and components with "non-standard encryption"
  - WLAN Authentication and Privacy Infrastructure (WAPI)
  - Computer forensic and network forensic
  - More aggressive network penetration items are in B2
- Requires encryption registration
- Authorizes export to non-government end-users and government end-users located in all countries except embargoed/terrorist designated countries (Crimea region of Ukraine, Cuba, Iran, North Korea, Sudan & Syria)

Supplement No. 3 to Part 740

SUPPLEMENT NO. 3 TO PART 740 - LICENSE EXCEPTION ENC FAVORABLE TREATMENT COUNTRIES

Australia
Austria
Belgium
Bulgaria
Canada
Cyprus
Czech Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Iceland
Ireland
Italy
Japan
Latvia
Lithuania
Luxembourg
Malta
Netherlands
New Zealand
Norway
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
Turkey
United Kingdom

Note 3 and Note 4: Encryption Items

- Encryption items controlled in Category 5, Part 2:
  - Note 3 items ("mass market")
- Encryption items not controlled in Category 5, Part 2:
  - Note 4 items (formerly known as "ancillary" encryption)

Note 3 – Mass Market

- Hardware and software described in Note 3 to Category 5, Part 2, Information Security – Cryptography Note
  - Origins in the General Software Note – GSN
  - Items widely distributed and certain components of those items
- If meet criteria, controlled under ECCN 5X992 – released from ECCN 5X002

Note 3 – Mass Market

- Note 3 describes mass market as:
  - Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
  - Over-the-counter transactions;
  - Mail order transactions;
  - Electronic transactions; or
  - Telephone call transactions;
  - The cryptographic functionality cannot be easily changed by the user;
  - Designed for installation by the user without further substantial support by the supplier; and
  - When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority [WA member implementation, e.g., US authorities] in the exporter's country in order to ascertain compliance described in paragraphs (1) through (3) of this note

Note 3 – Mass Market

- Transfers of mass market items with bit strengths greater than 64 bits require encryption registration with BIS
- Lower strength mass market products may be self-classified as 5x992
  - Key lengths not exceeding 64 symmetric; 768 asymmetric; or
  - 128 elliptic curve
- Higher strength mass market products may require BIS classification

Note 4 – Formerly "Ancillary" Encryption

- Excludes many items from Category 5, Part 2 based on their functionality
- If Note 4 applies, the CCL classification (e.g., EAR99, 5A991) is the classification the item would have without encryption

Note 4 – Formerly "Ancillary" Encryption

Wassenaar Arrangement (WA) Note 4 language included in the EAR:

Category 5–Part 2 does not apply to items incorporating or using "cryptography" and meeting all of the following:

a. The primary function or set of functions is not any of the following:
   1. "Information security";
   2. A computer, including operating systems, parts and components therefor;
   3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or
   4. Networking (includes operation, administration, management and provisioning);

b. The cryptographic functionality is limited to supporting their primary function or set of functions; and

c. 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 a. and b. above.

Note 4 – Formerly "Ancillary" Encryption

- BIS 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

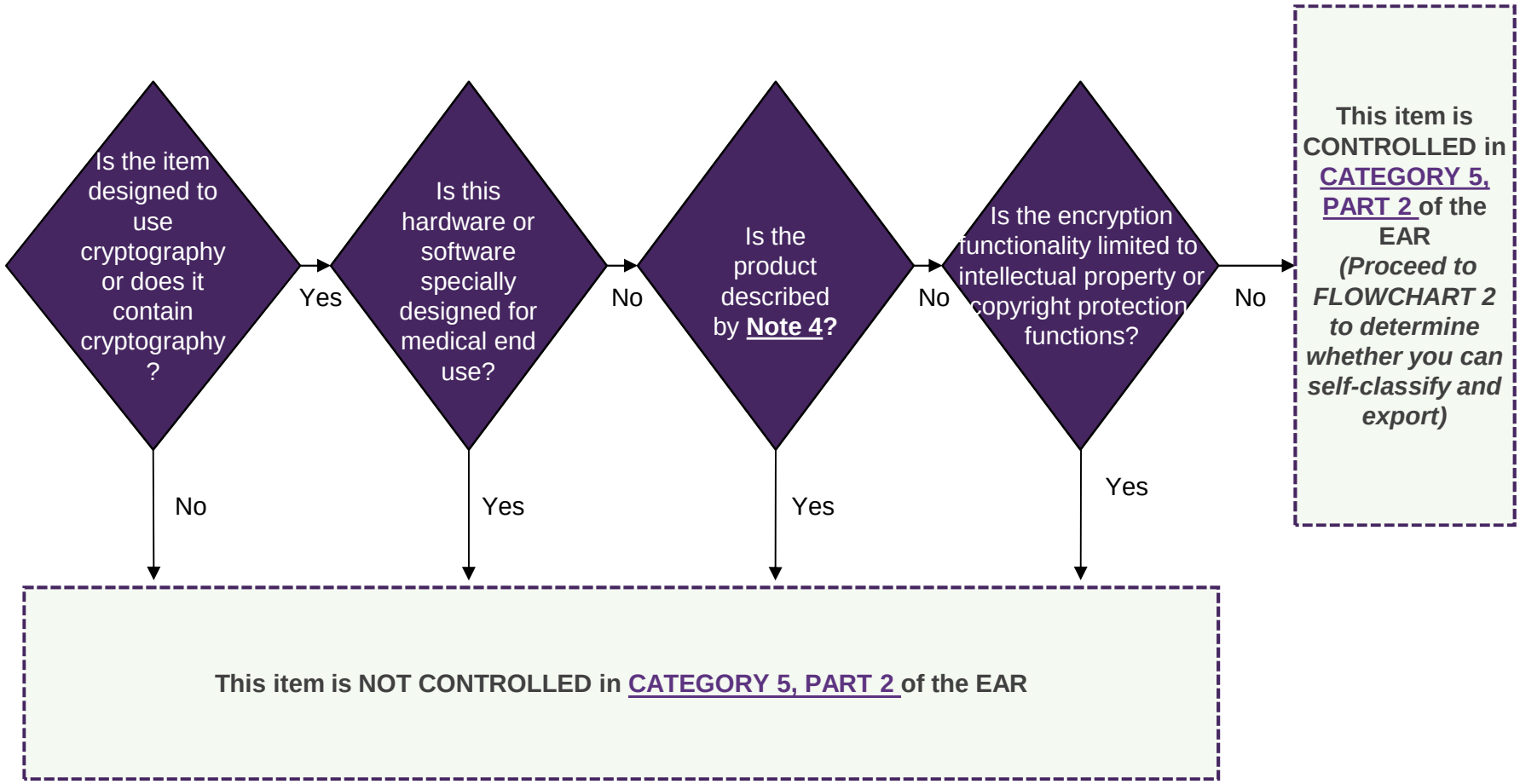
Note 4 – Formerly "Ancillary" Encryption

- BIS examples of items excluded from encryption
  - controls by Note 4
  - 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

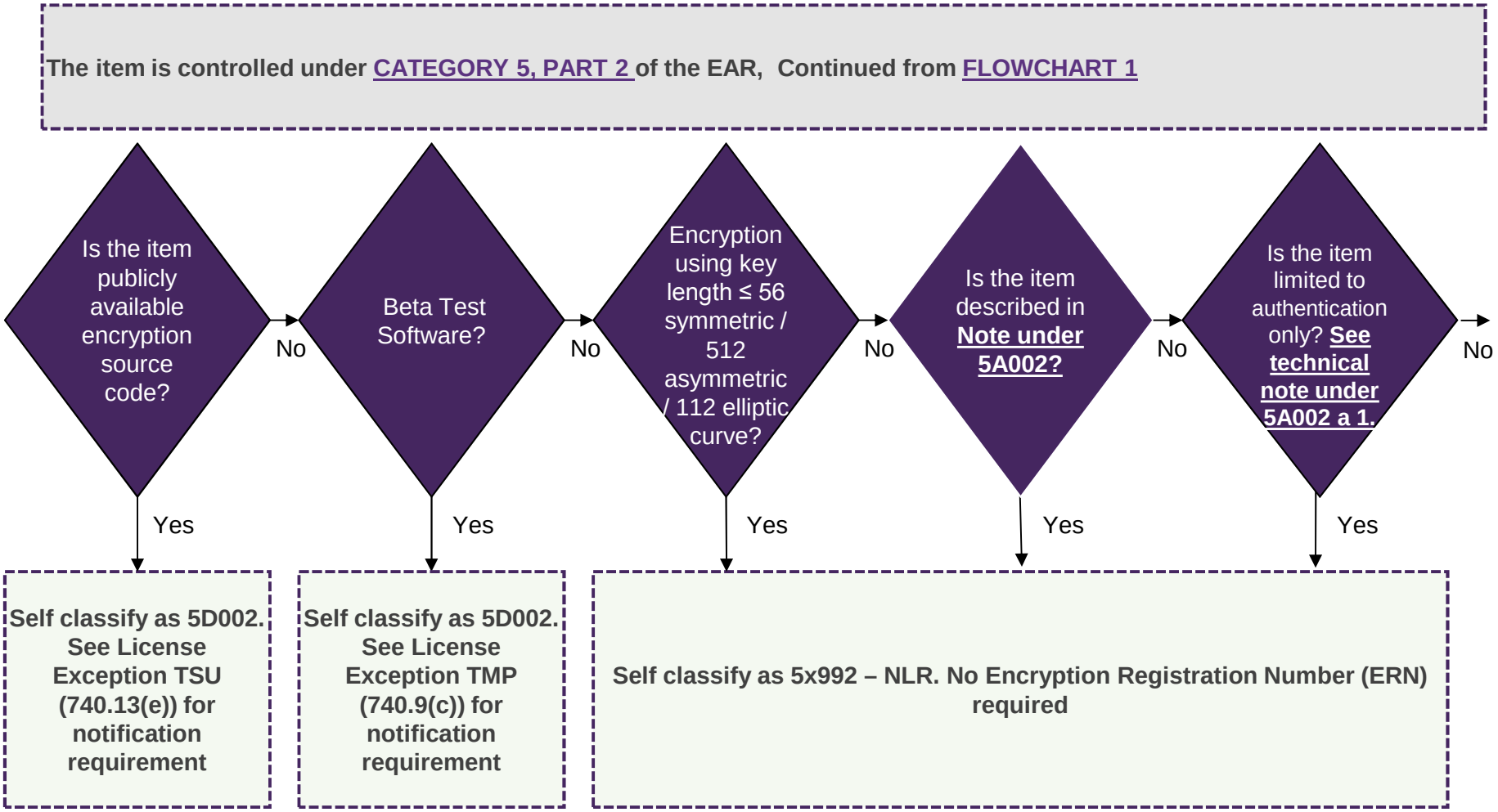
Note 4 – Formerly “Ancillary” Encryption

- Not primarily useful for computing (including the operation of "digital computers"), communications, networking (includes operation, administration, management and provisioning) or "information security“
- Interpreting Note 4 is difficult
- BIS examples are helpful yet broad categories

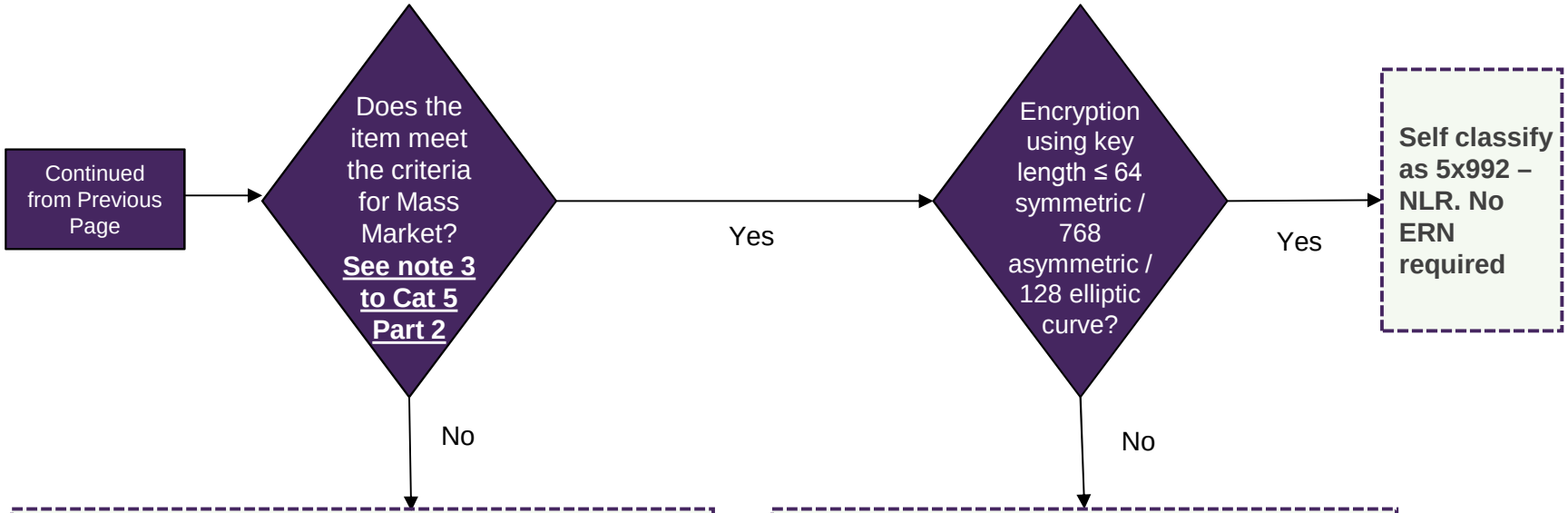
BIS Flow Chart 1: Items Designed to Use Encryption NOT Controlled Under CATEGORY 5, PART 2 of the EAR



BIS Flow Chart 2: Classifying under an ECCN in Category 5, Part 2



BIS Flow Chart 2 (continued)



ECCN5x002

X = A (hardware), B (test equipment), D (software), or E (technology)
Use License Exception ENC (740.17)

- **If 740.17 (a)(1), (a)(2), or (b)(4) – self classify as 5x002 / no ERN required**
- **If 740.17(b)(1) – self classify as 5x002 / ERN required**
- **If 740.17(b)(2) or (b)(3) – Submit 30 day ENC classification request / ERN required**

- Other license exceptions available for export of 5x002 include TMP, BAG, GOV, LVS

ECCN5x992

X = A (hardware), B (test equipment), D (software), or E (technology)
Use 742.15 of EAR – Mass Market Encryption

- **If 742.15(b)(4) – self classify as 5x992 / no ERN required**
- **If 742.15(b)(1) – self-classify as 5x992 / ERN required**
- **If 742.15(b)(3) – submit 30 day Mass Market classification request / ERN required**

Reporting Requirements

- Types of Reporting:
  - Annual Self-Classification Report
  - Semi-Annual Sales Reporting
- Type of reporting based on control status
- Note 3: Manufacturers/exporters who are registered can self-classify qualifying mass market items (Note 3) and immediately export most encryption products (with certain exceptions)
  - Review applicability of Annual Self-Classification Report
- Note 4: No reporting requirements if the product falls within the scope of Note 4

ANNUAL SELF-CLASSIFICATION REPORT

Self Classification

Note 3

- Lower strength encryption -<64-bit mass market: self-classification as 5X992 and no encryption registration
- Higher strength encryption - >64-bit mass market described in 742.15(b)(1): self-classification as 5X992 with an encryption registration
- Self-classification not available for certain specified mass market items - described in 742.15(b)(3)
  - Registration requirement as well

Note 4

- Eligible for self-classification

Self-Classification Report: How to Submit

- Report must be:
  - submitted as an attachment to an e-mail to BIS and NSA
  - in tabular or spreadsheet form, in comma separated values format (.csv)
- Must specify the export timeframe that the report spans and identify point of contact to whom questions or other inquiries from BIS or NSA pertaining to the report should be directed
- Identify email with subject line "Self-classification report for ERN R######"

Self-Classification Report: What to Report – Supplement No. 8 to EAR § 742

- For each encryption item, must report:
  - Name of product
  - Model / series / part number (if necessary, enter "NONE" or "N/A")
  - Primary manufacturer (enter "SELF" if you are the primary manufacturer)
  - Export Control Classification Number (to 5-digit level only, e.g., "5D002")
  - Encryption authorization type identifier: ENC or MMKT
  - Item type descriptor (selected from among 49 possibilities listed in Supplement No. 8 to Part 742 – Self-Classification Report for Encryption Items)

SUPPLEMENT NO. 8 TO PART 742 - SELF-CLASSIFICATION REPORT FOR ENCRYPTION ITEMS

This supplement provides certain instructions and requirements for self-classification reporting to BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD) of encryption commodities, software and components exported or reexported pursuant to encryption registration under License Exception ENC (§ 740.17(b)(1) only) or 'mass market' (§ 742.15(b)(1) only) provisions of the EAR. See § 742.15(c) of the EAR for additional instructions and requirements pertaining to this supplement, including when to report and how to report.

(a) Information to report

The following information is required in the file format as described in paragraph (b) of this supplement, for each encryption item subject to the requirements of this supplement and §§ 740.17(b)(1) and 742.15(b)(1) of the EAR:

(1) Name of product (50 characters or less.)

(2) Model / series / part number (50 characters or less.) If necessary, enter 'NONE' or 'N/A'.

(3) Primary manufacturer (50 characters or less.) Enter 'SELF' if you are the primary

(5) Encryption authorization type identifier, selected from *one* of the following, which denote eligibility under License Exception ENC (§ 740.17(b)(1), only) or as 'mass market' (§ 742.15(b)(1), only)

(i) ENC
(ii) MMKT

(6) Item type descriptor, selected from one of the following:

(i) access point
(ii) cellular
(iii) computer
(iv) computer forensics
(v) cryptographic accelerator
(vi) data backup and recovery
(vii) database
(viii) disk / drive encryption
(ix) distributed computing
(x) e-mail communications
(xi) fax communications
(xii) file encryption
(xiii) firewall
(xiv) gateway
(xv) intrusion detection
(xvi) key exchange
(xvii) key management

Self-Classification Report: Where to Report

- BIS: crypt-supp8@bis.doc.gov
- ENC Encryption Request Coordinator: enc@nsa.gov

Self-Classification Report: When to Report

- For encryption commodities, software and components exported or re-exported during calendar year (Jan 1 – Dec 31), report must be received by BIS and NSA no later than Feb 1 of the following year
- If no info has changed since previous year's report, can send e-mail stating that nothing has changed since the previous report
- No report is required if no exports or re-exports of applicable items were made during the calendar year

SEMI-ANNUAL SALES REPORTS

Semi-Annual Sales Reports: What to Report

- Required for exports to all destinations other than Canada, and for re-exports from Canada ONLY for items described under 740.17(b)(2) and 740.17(b)(3)(iii)
- Must report the following:
  - CCATS number
  - Name of item(s) exported (or re-exported from Canada)
  - For items exported (or re-exported from Canada) to a distributor or other reseller, must report their name and address, the item and quantity exported or re-exported, and (if known) the end user's name and address (cont'd)

Semi-Annual Sales Reports: What to Report (cont'd)

- For items exported (or re-exported from Canada) through direct sale, must report the recipient's name and address, the name of the item, and the quantity exported
- For exports or direct transfers of encryption components, source code, general purpose toolkits, technology, or items that provide an "open cryptographic interface" to a foreign developer or manufacturer in a non-Supplement 3 country when intended for use in foreign products developed for commercial sale, must report the names and addresses of the manufacturers, and (if known) when the product is made available for commercial sale, a non-proprietary technical description of the foreign products for which the encryption items are being used

Semi-Annual Sales Reports: When to Report

- For exports between Jan. 1st and June 30th, report is due no later than Aug. 1st of that year
- For exports between July 1st and Dec. 31st, report is due no later than Feb. 1st of the following year

Semi-Annual Sales Reports: Where to Report

- Reports must be in electronic format: spreadsheets, tabular text or structured text (may request other reporting arrangements with BIS to better reflect your business model)
- Send reports electronically to BIS at crypt@bis.doc.gov and to NSA at enc@nsa.gov, OR (see next slide)

Semi-Annual Sales Reports: Where to Report

- Reports on disks or CDs may be sent to:
  - Department of Commerce, Bureau of Industry & Security, Office of National Security & Technology Transfer Controls, 14th Street & Pennsylvania Ave, NW, Room 2705, Washington, D.C. 20230, Attn: Encryption Reports
  - Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Ft. Meade, MD 20755-6000

Semi-Annual Sales Reporting is Not required for …

- Encryption commodities or software with a symmetric key length not exceeding 64 bits
- Encryption items exported (or re-exported from Canada) via free and anonymous download
- Encryption items from or to a U.S. bank, financial institution, or its subsidiaries, affiliates, customers or contractors for banking or financial operations
- Foreign products developed by bundling or compiling of source code (cont'd)

Semi-Annual Sales Reporting is Not required for … (cont'd)

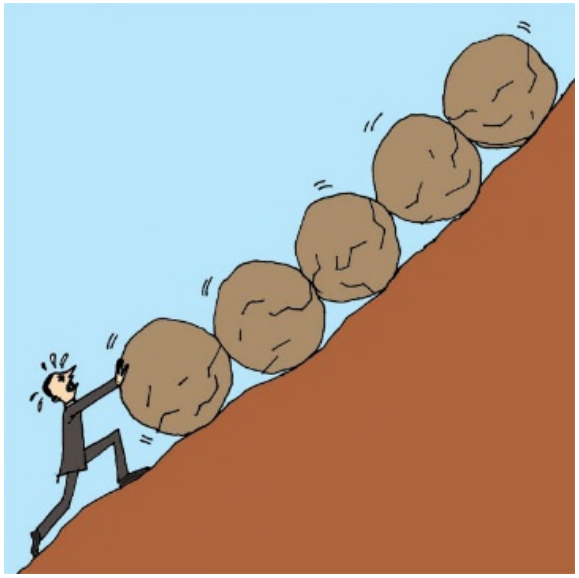
- Commodities and software that incorporate components or software that provide short range wireless encryption functions
- Foreign products developed with or incorporating U.S. origin encryption source code, components, or toolkits (with caveats)

Misconceptions

Misconceptions

- Encryption? What Encryption?”
- “It’s All Mass Market!”
- “We Only Use Open Source Encryption.”

Challenges/Compliance Risks



Acquisition

- Due diligence in the course of acquisition of a US or foreign entity
- Short turnaround time with limited access to documents in the data room, as buyer, on which to make a risk determination
- Encryption embedded in many product lines
- Lack of certainty in classification
- Certain encryption product lines may trigger national security-CFIUS issues
- Export control exposure is not generally the primary driver of decision making in acquisitions
- Successor liability

Third Party Component Classification

- Issues may arise when exporting/reexporting encryption products where you are not the product manufacturer
- BIS' FAQs indicate that exporters/reexporters that are not producers of the encryption item may rely on the: Encryption Registration Number (ERN), self-classification report, or CCATS that is published by the producer
- Vulnerabilities in that approach
- More vulnerabilities if the product manufacturer/OEM does not provide the classification information

Outsourced IT

- Location and nationality of IT service/service provider
- Invariably involves the use, sharing and/or exchange of encryption capable systems
- The parties' arrangements must satisfy requirements of all countries involved
- Companies not in the business of the manufacture of encryption products, e.g., financial, energy, steep learning curve to understanding and complying with encryption controls

Wassenaar (WA) Implementation

- International business exposes companies to many export control
- regimes
- WA control lists are published and available
- http://www.wassenaar.org/
- While WA lists are mutually agreed to, interpretation and implementation are not the same under (or due to) national discretion principles
- Operational challenges in light of inconsistent application among governments, e.g., treatment of Notes 3 and 4 products
- Non-WA country encryption controls pose additional challenges for an already complicated landscape

Final Thoughts

- Encryption excluded from controls under Category 5, Part 2, may be controlled under other ECCNs, e.g., communications
- The normal rules of the EAR regarding de minimis content do not apply to encryption
- EAR encryption adopts the "see through" rule akin to the ITAR
- Not all mass market products can be self-classified
- For encryption – open source is not necessarily treated as public domain/publicly available and therefore excluded from controls
  - US treatment (e.g., License Exception Technology and Software Unrestricted (TSU) – EAR 740.13-type source code)
  - Some countries more restrictive than US

QUESTIONS ?

Speakers

Margaret M. Gatti
Washington, DC
T +1.202.739.5409
margaret.gatti@morganlewis.com

Margaret Gatti represents US and non-US companies, universities, and financial institutions in matters involving economic sanctions, export controls under the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR), customs and import regulations, free trade agreements, antiboycott regulations (EAR and IRS), anticorruption laws (FCPA and UKBA), anti-money laundering legislation, international commercial sales terms (INCOTERMS), international e-commerce, and Bureau of Economic Analysis (BEA) reporting, as well as national security issues.

Speakers

Marynell DeVaughn
Washington, DC
T +1.202.739.5863
marynell.devaughn@morganlewis.com

Marynell DeVaughn represents US and international clients in national security and international trade law matters, such as counseling clients on the Export Administration Regulations (EAR), encryption export controls and regulations, International Traffic in Arms Regulations (ITAR), economic sanctions and trade embargoes administered by the Office of Foreign Assets Control (OFAC), Foreign Corrupt Practices Act and anticorruption, military exports and defense offsets, antiboycott regulations, and the Committee on Foreign Investment in the United States. She advises clients on relevant laws and regulations; development and assessment of company compliance policies and programs; internal and government investigations; compliance assessments and audits; voluntary disclosures to appropriate government authorities; and commodity jurisdiction, licensing, and administrative enforcement issues.

THANK YOU