Strafford

Presenting a live 90-minute webinar with interactive Q&A

International Encryption Control: Navigating Differing Regulations and Exceptions

Overcoming Licensing and Classification Challenges and Implementing a Global Compliance Program

TUESDAY, AUGUST 19, 2014

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Thaddeus R. McBride, Partner, **Sheppard Mullin Richter & Hampton**, Washington, D.C.

Martina de la Torre, Sr. Manager, Global Trade Compliance, **Symantec**, Mountain View, Calif.

Bill Vawter, Manager, Trade Compliance, **Symantec**, Mountain View, Calif.

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 10**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-866-570-7602** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

For CLE purposes, please let us know how many people are listening at your location by completing each of the following steps:

- In the chat box, type (1) your **company name** and (2) the **number of attendees at your location**
- Click the SEND button beside the box

If you have purchased Strafford CLE processing services, you must confirm your participation by completing and submitting an Official Record of Attendance (CLE Form).

You may obtain your CLE form by going to the program page and selecting the appropriate form in the PROGRAM MATERIALS box at the top right corner.

If you'd like to purchase CLE credit processing, it is available for a fee. For additional information about CLE credit processing, go to our website or call us at 1-800-926-7926 ext. 35.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

Encryption Export Controls: Navigating Differing Regulations

Strafford Publications Webinar

August 19, 2014

Thaddeus R. McBride

Sheppard Mullin Richter & Hampton

Martina de la Torre

Bill Vawter

Symantec

SheppardMullin

Symantec

Agenda

- Introduction
- Overview of US encryption controls
- Chinese and other non-US controls
- Compliance Strategies
- Questions

Vigorous Enforcement

- Civil fines
- Criminal fines
- Imprisonment
- Denial of export privileges

Encryption Background

- What is encryption?
  - Used to maintain secrecy of data
  - Protect against security breaches
  - May be hardware or software

Encryption Background

- How controlled?
  - Controlled by US Commerce Department, Bureau of Industry & Security (unless specifically designed for military / space application)
  - Export Administration Regulations (EAR)

Background (cont'd)

- Why controlled?
  - Protect national security
  - Preserve US technology advantages
  - Previously controlled under the ITAR

Relevant Regulatory Provisions

- EAR Part 774, Supplement 1 – Commerce Control List
  - Encryption items covered by Category 5, Part 2
  - CCL spells out whether license is required for particular country

Regulatory Provisions (cont'd)

- EAR Part 742.15 – Encryption Items
  - Licensing Requirements
  - Registration Requirements
    - Mass Market Treatment
  - Self-classification reporting
  - Grandfathering of previously classified *mass market* products

Regulatory Provisions (cont'd)

- EAR Part 740.17 – License Exception ENC
  - Principal License Exception available for encryption products
    - Some notification requirements; in other cases, no notification required
    - 30-day wait may be necessary too
    - Some semi-annual reporting requirements

Regulatory Provisions (cont'd)

- EAR Part 740.13 – License Exception TSU
  - Another License Exception available for encryption products
    - For open source / community source encryption
    - Exception generally available if underlying export is permitted

Other Regulatory Provisions

- License Exceptions BAG and TMP (part 740)
- Special *de minimis rules* (part 734.4)
- Unique definition of “export” for certain encryption exports (part 734.2)

Encryption Classification

- Does hardware / software use or contain cryptography?
  - If no, not controlled for ENC purposes
  - If yes, continue analysis and recognize exceptions:
    - Medical use?
    - Eligible for self-classification?
    - Exports to a foreign affiliate?
    - Other?

Encryption Licensing

- When no prior review for ENC has been performed
- Certain high-level encryption items
- Cryptanalytic items to government end users
- Exports to E:1 countries

Chinese and Other Non-US Controls

SheppardMullin

Symantec

General Concepts

- "Import" versus "use" encryption controls
  - Determines who is responsible for licenses
- "Registration" versus "testing" encryption controls
- Regulations may stem from different government organizations with concurrent jurisdiction
  - Defense
  - Customs
  - Law enforcement/state security/intelligence agencies
  - Information security/technology agencies
  - Special purpose encryption control agencies

Jurisdictions

- Most aggressively regulating encryption imports: China, France, Hong Kong, Israel, and Russia
- Many others do not actively enforce restrictions (*e.g.*, South Africa)
- Country information resources
  - Steptoe and Johnson LLP (InternatLaw LLC) offers a country-by-country guide subscription service
  - Local country legal counsel and embassies
  - Crypto Law Survey (http://www.cryptolaw.org/)
    - Not authoritative

Israeli Import Controls

- Restricts import and use of encryption hardware, software (tangible and intangible), and technology
- Controls administered by Israeli Ministry of Defense
- Few exceptions, except for internal business or personal use
  - Encryption products subject to inspection and seizure
- Licensing is a simple process that typically takes less than 30 days
  - Application must disclose encryption algorithms

Hong Kong Import Controls

- Restricts encryption import (not use)
- Controls administered by HK Trade and Industry Department and enforced by HK Customs
- Exemptions
  - Intangible transfers/electronic software delivery
  - Authentication only products (ECCN 5D992.b)
  - Mass market encryption products (ECCN 5D992.c)
  - HK is not a Wassenaar signatory, but issues other exceptions in line with the Arrangement

French Import Controls

- Tightly controls encryption import and supply to third parties, but not use
- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) issues licences
  - May require source code or samples
  - Applications must be in French, local counsel recommended
  - At least one month processing time

French Controls (cont'd)

- Exemptions
  - Many mass market (ECCN 5D992.c) products remain controlled
  - Both tangible and intangible transfers remain controlled
  - Authentication-only and "products using encryption only for administration, management or configuration of a computer system" are exempt
    - ANSSI is primarily concerned with encryption of end-user messages and documents both at rest and in transit.
    - Control Plane (infrastructure) versus Data Plane (user information)
    - Vague and sometimes difficult to apply in practice

Russian Import Controls

- Broad controls on import, use, distribution, maintenance, and development of encryption products
- Administered with great discretion by the Federal Security Service (FSB) and Ministry of Industry and Trade (MIT)
  - Legislation grants concurrent jurisdiction
  - FSB controls the process and must grant permission before license application can be submitted to MIT
  - Local counsel recommended to monitor application process

Chinese Regulatory Environment

- Government officials and ministries view regulations as public statements of their enforcement intent
- Government often communicates desired policy outcomes through unofficial channels
- Public sector is a unique ecosystem with multiple, sometimes conflicting power bases
  - National, regional, provincial, and local governments can all exert independent authority

Chinese Environment (cont'd)

- Policies and enforcement patterns can change unexpectedly with limited official explanation of policy evolution or rationale
- Regulatory process does not constrain policy outcomes
- No independent judiciary to adjudicate disputes with regulators

Chinese Environment (cont'd)

- Constraints on government discretion
  - Individual officials or less influential ministries constrained by the policy decisions of more powerful government entities
    - Tendency toward relative uniformity
  - If regulatory controls are too unpredictable they will discourage foreign investment
  - Foreign companies may be the best supplier of a particular product, with no competitive domestic replacement

Chinese Environment (cont'd)

- Government wields substantial power as China's largest single customer
  - State controls estimated 50 percent of total GDP as a market participant
  - Complete control of "vital sectors" such as banking and infrastructure
  - Influential ministries can take companies or specific products off of their acceptable purchase list
    - Can create a chilling affect across the public sector

Chinese Import Controls

- Due to regulatory environment, ongoing communication with the government is critical for interpreting controls
- Two primary government entities with relatively independent jurisdiction
  - State Encryption Management Bureau (SEMB)
  - Ministry of Public Security (MoPS)

Chinese Controls (cont'd)

- SEMB controls products with encryption as "core function"
  - Chinese entities and citizens are forbidden to use these products
  - Only Foreign Invested Entities (FIEs) or foreign individuals may use encryption products after they obtain a permit from SEMB
    - No permit required for foreign company to sell to FIE, but importer should implement screening process

Chinese Imports (cont'd)

- MoPS controls products that have information security functionality, but do not have encryption as core function
  - Focus is more on consumer protection for open sale
- Importer must first identify MoPS category code and test standard
- Importer must work with MoPS to test product against criteria
- MoPS will issue test certificate and license
- Stickers may be required for physical products

Compliance Strategies

SheppardMullin

Symantec.

Comply with Global Controls

- Take steps to ensure compliance with US encryption control laws and encryption laws of other countries
  - Investigate encryption regulations of other countries
    - Laws that regulate encryption may be “use”, sales, import, or export control (dual-use) related
    - Manufacturers comply with, France, Israel, China regulations
    - Manufacturers/Importers can comply with
      - Russia regulations related to import of products containing encryption
      - Hong Kong import registration requirements

Communicate Classification Information

- Communicate export control information to your internal customers: sales, marketing, shipping and to third party fulfillment partners
- Post information to be used by your external customers
  - Export Control Classification Numbers (ECCN)
  - EAR Paragraphs (740.17.b.1, for example)
  - Commodity Classification Tracking System number CCATS
  - List relevant Authorization types: MMKT, ENC, NLR

Steps to Ensure Global Compliance

- Once you have classified your products….
  - Assign appropriate export or import classification numbers, codes/attributes to your products, items or skus in your Product or SKU master
  - Assign/append the classifications from all countries, the import approval numbers and information regarding other country approvals
    - Expiration/renewal dates

Compliance Steps (cont'd)

- Assign/append flags/indicators related to
  - Encryption classifications to help you identify transactions (using such products) that will subsequently need to be reported or that might need an export license
  - Customer records to support encryption definitions related to "government", military, police, state security, commercial, or academic type "customers/end users"

Steps to Ensure Licensing Compliance

- Supplement No. 3 to Part 740 – License Exception ENC, Favorable Treatment Countries

- Transactions for End Users in countries not included in Supplement No. 3
  - Ensure that products classified as 5X002, EAR 740.17.b.2 will not be sold under License Exception ENC to Government (Military or Police) end users in countries not included in Supplement No. 3 to Part 740
    - Obtain export license for transactions that do not qualify under the terms and conditions listed under 740.17.b.2

Licensing Compliance (cont'd)

- Invest in a trade compliance screening system/solution to help you:
  - Identify and stop transactions that may require an export license based on ECCN and / or End User
    - Government
    - Military
    - Police/State Security
  - Identify transactions that may need to be reported to relevant government authorities
    - Government, Commercial, Private, Academic
  - Manage Export Licenses

Government Reports

- Ensure you comply with relevant reporting obligations for your exports and re-exports
  - US ENC Report for 740.17(b)(2) and 740.17(b)(3)(iii)
    - Semi-annual reporting is required for exports to all destinations other than Canada
  - Singapore License Reporting
  - Other Global License/Open License Reports – EU
- US annual self-classification report
  - Items exported under ENC - 740.17(b)(1)
  - Items exported under Mass Market - 742.15(b)(1)

US Re-Export Controls

- US Re-export controls
  - Ensure that if your US origin product, technology or software, subject to the EAR, will be exported or re-exported from another country, such export or re-export will comply with US encryption-related export licensing controls
    - Any controls that apply to exports also apply to re-exports!
  - Reporting requirements apply to all re-exports, including re-exports from Canada!

Thank You!

Thaddeus R. McBride
Sheppard Mullin Richter & Hampton
TMcBride@sheppardmullin.com

Martina de la Torre
Symantec
martina_delatorre@symantec.com

Bill Vawter
Symantec
Bill_Vawter@symantec.com

SheppardMullin

Symantec