Export Controls and Encryption

Anita Zinzuvadia, BIS
Brittany Whiting, UCSD

Impact of Export Controls on Higher Education and Scientific Institutions
May 23-24, 2016
Agenda

• Jurisdiction:
  – State-ITAR vs. Commerce-EAR Dual Use
    • We are only covering Commerce encryption regulatory requirements in this session
• Subject within the scope of the EAR?
• Encryption Classification
• License Exceptions
• Registration, CCATS, Reporting Requirements, licensing
Within Scope of EAR-Subject?

• What is being exported?
  – Item, software or technology

• Is it excluded from the regulations?
  – Fundamental research (734.8)
  – Published information and software (734.7)
  – Educational information (734.9)
  • But not for 5D002 except when meeting publicly available object code under 740.13 (e)
Special Considerations for Exclusions

• Does not cover certain encryption...
• Ex. Access to encryption source code may be part of tool development
Impact to Research

• Foreign person and/or international collaborations participation in certain information security development
• Industry collaborations with proprietary encryption code
• Exports and hand carries of equipment for international research
What Are Encryption Items?

- Software and Hardware that implement symmetric & asymmetric encryption algorithms like AES, DES, Diffie Hellman, RSA
- Smartphones, routers, gateways, firewalls, network infrastructure and switches, telecom infrastructure
- Operating systems, laptops or mobile devices may have encryption
- Software that makes calls to third-party encryption libraries
Exit Strategy Options

• Navigate the maze of encryption controls to see if you can exit without a license through a path of decontrol, exemption or a license exception
FLOW CHART 1: ITEMS DESIGNED TO USE ENCRYPTION
NOT CONTROLLED UNDER CATEGORY 5, PART 2 OF THE EAR

Is the item designed to use cryptography or does it contain cryptography?
Yes

Is this hardware or software specially designed for medical end use?
Yes

Is the product described by Note 4?
Yes

Is the encryption functionality limited to intellectual property or copyright protection functions?
Yes

This item is controlled under CATEGORY 5, PART 2 OF THE EAR

(Proceed to Flow Chart 2 to determine whether you can self-classify and export)

This item is not controlled in CATEGORY 5, PART 2 OF THE EAR
Category 5 Part 2 Does Not Cover

- Medical end use
- Encrypted data
- Compression
- Fixed coding techniques like CDMA
Note 4: 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 completely removes the decontrolled items from control under Category 5, Part 2 of the CCL.

• Please note that certain products may be controlled under an ECCN elsewhere in the CCL even if they are no longer controlled for encryption reasons.
Classification for Encryption

- EAR99
- 5X992 – Anti-Terrorism (AT) control
  - key length is less than 56 bits for symmetric encryption, less than 512 for asymmetric or 112 elliptic.
  - item is using encryption for authentication only
  - Related control notes
- 5X992 Mass market
- 5X002 National Security and AT
- Others depending on item
License Exceptions

• TSU (740.13) - Technology & Software Unrestricted
  – Open source, Published software
• ENC (740.17) - Encryption Commodities, Software and Technologies
• TMP (740.9) - Temporary exports
• BAG (740.14) - Baggage
FRE Example

• Iranian national working on fundamental research in computer science
• As part of his research he requires access to AES encryption code
• Is this covered by the FRE?
• If not, is it covered by TSU or ENC?
# Mass Market Encryption

## MASS MARKET ENCRYPTION (Sec. 742.15) SUMMARY -- September 2015

<table>
<thead>
<tr>
<th>742.15 Sub¶</th>
<th>ITEM DESCRIPTION OR PURPOSE OF EXPORT</th>
<th>ECCN</th>
<th>END USERS AUTHORIZED</th>
<th>SUBMISSION REQUIREMENTS</th>
</tr>
</thead>
</table>
| (b)(1)     | All items not described in 742.15(b)(3) or (b)(4) | 5A002.a1, a2, a5, a6, a9, 5B002, 5D002 -- Decontrolled to 5A992.c or 5D992.c | Govt. and non-govt. end users in all countries except E:1 and Cuba | 1. Encryption Registration (submit Supp. 5, part 742, in SNAPR)  
2. Annual Self-Classification Report (submit Supp. 8, part 742, by email) |
| (b)(3)     | (i) Encryption components: chips, electronic assemblies, crypto libraries, toolkits, dev kits  
(ii) Non-standard crypto items  
(iv) mass market cryptographic enabling items | 5A002.a1, a2, a5, a6, 5A002.b, 5D002 -- Decontrolled to 5A992.c or 5D992.c | Govt. and non-govt. end users in all countries except E:1 and Cuba | 1. Encryption Registration (submit Supp.5, Part 742 in SNAPR)  
2. Classification request (submit Supp. 6, part 742, in SNAPR) |
| (b)(4)     | (i) Short-range Wireless  
(ii) Foreign dev with US enc parts | 5A002.a1,5,6; 5B002; 5D002 decontrolled to 5A/D992.c | Govt. and non-govt. end users in all countries except E:1 and Cuba | None |
Travel Abroad with Laptop

• Does the laptop have any export restricted encryption software or technology?
  – Many manufacturers indicate classification
    • Windows 10, 5D992 Mass market
    • Red Hat Enterprise Linux 7.x, 5D002 ENC Unrestricted 740.17(b)(1) CCATS G154202
  – Is a license required?
## License Exception ENC (Section 740.17) Summary -- September 2015

<table>
<thead>
<tr>
<th>Subj</th>
<th>Item Description or Purpose of Export</th>
<th>ECCN</th>
<th>End Users Authorized</th>
<th>Submission Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>(a)(1)</td>
<td>Development/Production Only</td>
<td>5A002.a1, a2, a5, a6, a9, 5A002.b, SB002, SD002, SE002</td>
<td>Private end user HQ'd in a Supp. 3 country (wherever located except E:1/Cuba)</td>
<td>None</td>
</tr>
<tr>
<td>(a)(2)</td>
<td>Any internal purpose</td>
<td>5A002.a1, a2, a5, a6, a9, 5A002.b, SB002, SD002, SE002</td>
<td>U.S. subsidiaries (also employees, interns, contractors, except E:1/Cuba)</td>
<td>None</td>
</tr>
</tbody>
</table>
| (b)(1) | All items not described in (b)(2), (b)(3) or (b)(4) | 5A002.a1, a2, a5, a6, a9, SB002, SD002 | Govt. and non-govt. end user in all countries except E:1 and Cuba | 1. Encryption Registration (submit Supp. 5, part 742, in SNAPR)  
2. Annual Self-Classification Report (submit Supp. 8, part 742, by email) |
| (b)(2) | Network infrastructure, source code, designed for govt', custom crypto, modifiable crypto, quantum crypto, penetration testing, public safety radio, cryptanalytic, OCI, technology (standard and non-) | 5A002.a1, a2, a5, a6, a9, 5A002.b, SB002, SD002, SE002 | Govt. end users in Supp. 3 and non-govt. end users in all but E:1 and Cuba  
**Cryptanalytic:** non-govt. end users in all but E:1 and Cuba  
**OCI:** govt and non-govt in Supp. 3  
**SE002:** non govt end user in all but D:1 (unless HQ in Supp. 3), E:1 and Cuba (except non-standard/cryptanalytic) | 1. Encryption Registration (submit Supp.5, Part 742 in SNAPR)  
2. Classification request (submit Supp. 6, part 742 in SNAPR)  
3. Semi-Annual Sales Report by email (see 740.17(e)) |
| (b)(3) | (i) Encryption components: chips, electronic assemblies, crypto libraries, toolkits, dev kits  
(ii) Non-standard crypto items  
(iii) Digital forensics  
(iv) Cryptographic enabling items | 5A002.a1, a2, a5, a6, 5A002.b, SD002 | Govt. and non-govt. end users in all countries except E:1 and Cuba | 1. Encryption Registration (submit Supp.5, Part 742 in SNAPR)  
2. Classification request (submit Supp. 6, part 742 in SNAPR)  
3. Semi-Annual Sales Report for (b)(3)(iii) only (see 740.17(e)) |
| (b)(4) | (i) Short-range Wireless  
(ii) Foreign dev with US enc parts | 5A002.a1, a5, a6, SB002, SD002 | Govt. and non-govt. end users in all countries except E:1 and Cuba | None |
SNAP-R Encryption Registration

• Registration is required for (b)(1), (b)(2), and (b)(3) items under both ENC and mass market
• Complete the SNAP-R module "encryption registration"
• Attach Supplement 5 answers to Part 742
• Submit
• System will send the encryption registration number (ERN)
Encryption Classification

• Classification is required for items in (b)(2) and (b)(3) of ENC, and mass market (b)(3).

• Fill out the same commodity classification form in SNAP-R & attach a data sheet or equivalent, provide Supplement 6 answers on encryption functionality.

• Submit SNAP-R Classification Request
  – once submitted, you can start exporting immediately to the Supplement 3 countries
  – 30 days later, you can start exporting under the full authorization of ENC, even if BIS hasn’t issued the classification yet.
Reporting Requirements

- ENC in mass market two types of reporting requirements.
- Semi-annual sales report, required for the (b)(2) & (b)(3)(iii) items.
  - (b)(2) – network infrastructure, source code, pen test, Tetra
  - (b)(3)(iii) – forensic & packet inspection network analysis products
- Annual self-classification report required for all (b)(1) items exported under your own encryption registration number.
Encryption Export Licensing

- 5A002 and 5D002 described under ENC (b)(2) require license to govt’ end user outside Supp. 3 countries
- 5E002 - in addition to above, non-gov’t end user in D:1 countries require a license
- 5X992- E group countries, restricted entities, restricted end uses
Industry Collaboration Example

• 5E002 (NS1 & EI) technology from industry under a NDA
• Research team includes foreign person students & staff (CA, GB, IN, CN, IR)
• What are the deemed export license requirements?
• Are there any exceptions that can be used?
• What other questions need to be asked from the industry partner?
Other Considerations

• Exports licenses may be required from Foreign Countries to the US of encryption items

• Certain countries require import licenses for encryption items
  – Your research collaborator will need to have these in place to ensure no delays
Changing Regulations for Information Security

• WA 2015 rule – changes to ENC
• WA Intrusion Software in Cat. 4
• Cuba
• Changes in ITCD
QUESTIONS?