Encryption and Cyber Export Controls

BUREAU OF INDUSTRY AND SECURITY

U.S. DEPARTMENT OF COMMERCE

Part 1: Encryption - Category 5, Part 2

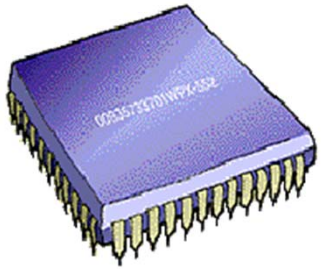
- What is in the Category? / What is not?
- License Exception ENC/ Mass market
- Publicly available
- Source code/technology

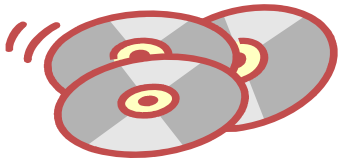
Do I have an encryption item?

5A002 controls products <u>designed</u> or <u>modified</u> to use encryption

This includes products that call encryption from an external source -- such as:

- operating system (OS) software
- external library
- third-party product
- cryptographic processor





5A002 a.1-a.4 Examples

- Products that have “information security” as a primary function include firewalls, intrusion detection systems, cryptanalytic tools, computer/network/digital forensics, cryptographic accelerators, file encryption, cryptographic libraries

- Digital communications or networking systems include routers, switches, base stations, trunked radio, wireless access points, bridges/repeaters, hubs, gateways, access points, modems, voice over internet protocol (VoIP) servers and endpoints

5A002 a.1-a.4 Examples

- Computers and other items having information storage or processing as a primary function include computers, mobile and handheld computers, processor chips, system on chips, boards, assemblies or other components of computers data backup and recovery, database, software development tools.

Technology and Source Code

5E002 – Encryption technology

5D002 – Encryption source code (published and unpublished)

Examples of Items Not Controlled under 5A002 a.1-a.4

Games and gaming devices

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

Examples of Items Not Controlled under 5A002 a.1-a.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

Not Described by the Decontrol Notes to 5A002.a

(a) Personalized smart cards and smart card readers, including RFID

(b) Equipment specially designed for money transactions or banking use

(f) Wireless “personal area network” (PAN) equipment

(h) Routers, switches, gateways or relays using encryption only for operations, administration or maintenance (OAM)

(i) Single board computers incorporating mass market processors or using a mass market operating system

(j) Certain IOT networking devices

License Exception ENC

Available for encryption items controlled for national security reasons except 5A003 and equivalent or related software and technology.

Requirements and authorization vary by

- Item
- End use
- End user

§ 740.17 License Exception ENC

CCATS	Reporting	Paragraph 740.17	End User Authorization (outside E-1)	Item Description or Purpose of Export
No	No	(a)(1)(i)	Companies HQ'd in Supp 3	Dev/Production[1]
No	No	(a)(1)(ii)	Subsidiaries of the same parent company HQ'd in Supp 3. country	Any internal purpose[1]
No	No	(a)(2)	U.S. Subs	Any internal purpose [1]
Yes	Yes	(b)(2)	license required for Gov't end users[2] not in Supp 3[3]; LE ENC for non-gov't end users[4]	(b)(2) commodity list
Yes	Yes for iii items only	(b)(3)	LE ENC to gov't and non-gov't end users	(b)(3) commodity list
No	Yes[5]	(b)(1)	LE ENC to gov't and non-gov't end users	not (b)(2) or (b)(3)

[1] All products developed are subject to the EAR.

[2] LE ENC available for network infrastructure to less sensitive gov't end user

[3] Supp 3 means end-users headquartered in Supp 3

[4] License also required for cryptanalytic to gov't end users in Supp 3; for any end user outside Supp 3 for OCI items and for special (OCI, non-std, cryptanalytic) technology and for std (other) technology to D-1 countries.

[5] Self-classification report required for certain items

Overview of Mass Market

- Mass market items have to meet Note 3 to Cat. 5 Part 2 (the mass market criteria)
- 740.17(b)(3) for “non-standard cryptography” or (b)(1) for most other mass market .
- Items described in 740.17(b)(2) and (b)(3)(iii) are not eligible for mass market
- Mass market items are classified under 5A992 and 5D992 instead of 5A002 and 5D002.

Mass market

ECCN/Authorization	Before March 29, 2021 rule	After March 29, 2021 rule
5x992.c –mass market items described in 740.17(b)(1) X= A for hardware or D for software	Fell under EAR Section 740.17(b)(1) -Required self-classification report or classification.	Falls under EAR Section 740.17(b)(1) - No self-classification report or classification required.
5x992.c – mass market chips, chipsets, electronic assemblies and field programmable logic devices (except for items implementing "non-standard cryptography")	Fell under EAR Section 740.17(b)(3) and required a classification.	Falls under EAR Section 740.17(b)(1) -- Require self-classification report or classification.
5x992.c – mass market cryptographic libraries, modules, development kits and toolkits (except for items implementing "non-standard cryptography")	Fell under EAR Section 740.17(b)(3) and required a classification.	Falls under EAR Section 740.17(b)(1) - No self-classification report or classification required.

https://www.bis.doc.gov/index.php/documents/pdfs/2759-table-of-changes-to-enc-in-wa2019-rule-final-version/file

Encryption items NOT subject to the EAR

- Items subject to the exclusive jurisdiction of another agency – e.g., ITAR.
- Certain "Publicly available" encryption software & source code (e.g., open source)

Note: While open source code itself may not be subject to the EAR, an item is not considered publicly available merely because it incorporates or calls to open source software.

“Published” and Encryption

5 ways that items in Cat. 5 Part 2 become publicly available:

If the item has **“non-standard cryptography”:**

1. Email notification if posting source code & corresponding object code
2. Classification request for mass market software made publicly available

"Published" and Encryption cont.

If the item ***does not*** have "non-standard cryptography"

3. No email notification required to make source code publicly available – treated just like any other source code under the EAR.
4. Mass market 'executable software' (i.e., firmware and see Note 3, Part b) under 740.17(b)(1) requires self-classification report or classification in order to be not subject.
5. Other types of mass market B1 items do not require any report or classifications – these items are treated just like any other item under the EAR.

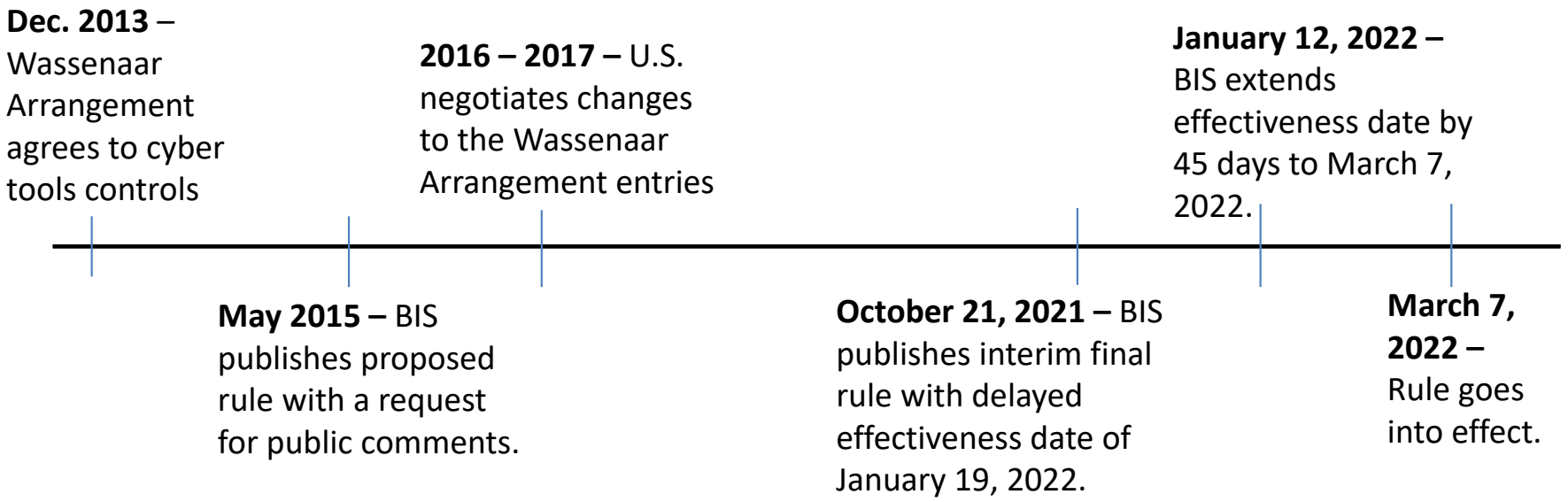
Example

- Item example
- Using third party encryption
- Making the item publicly available or mass market

Part 2: Cyber tools rule

- History
- What is subject
- Other relevant provisions
- License Exception ACE

Cyber Tool History



Cyber Tools

4A005 – Designed or modified for generation, command and control, or delivery of “intrusion software”

4D004 – Software specially designed for generation, command and control, or delivery of “intrusion software”

- Exception: Software update tools

4E001.c – Technology for the “development” of “intrusion software”

- Exception: “Vulnerability disclosure” and “cyber incident response”

Cyber Tools

5A001.j – intended to cover large scale government surveillance systems

- Must operate on a carrier class IP network and perform ALL of the following:
  - Analyze data at the application layer (OSI Layer 7);
  - Extract selected metadata and application content;
  - Index the data;
  - Execute searches of the indexed data based on “hard selectors”
  - Map the relational network of individuals or groups of people
- Does not apply to products specially designed for:
  - Marketing, QoS, QoE

Other Relevant Provisions

740.17(b)(2)(i)(F) – Penetration testing tools

5A004.a & 740.17(b)(2)(ii) – Cryptanalytic Items

5A980 - Devices primarily useful for the surreptitious interception of wire, oral, or electronic communications.

5A001.f.1 – Mobile telecommunications interception equipment.

Cyber Tools – LE "ACE"

Catch-all: Licenses required when the exporter "knows or has reason to know" that the item will be used for unauthorized (malicious) cyber activities

E:1/E:2: Licenses required for all E:1/E:2 exports including deemed exports, for any reason. Deemed export licenses **not** required for other foreign nationals

"U.S. subsidiaries", banks/financial, insurance, civil medical entities: No licenses required for any purpose.

Cyber Tools – LE "ACE"

Vulnerability Disclosure/Cyber Incident Response: No licenses required except for government end-users in D:1-D:5.

Government End-Users*: Licenses required to government end-users of D:1-D:5 countries.

- Exception 1: Exports to police and judicial bodies in Cyprus, Israel, and Taiwan of evidence of a cyber security incident for criminal or civil investigations or prosecutions.
- Exception 2: Exports to national CERTS in Cyprus, Israel, and Taiwan for vulnerability disclosure, cyber incident response, or criminal or civil investigations.
- Deemed Export licenses required.

*Definition differs from Cat. 5P2.

Cyber Tools – LE "ACE"

Non-government end-users: Licenses required to non-government end-users in D:1 or D:5 for purposes other than vulnerability disclosure and cyber incident response activities:

- Exception: U.S. subs, banks/finance, health/insurance, civil medical do not require a license for any reason.

Cyber Tools – LE "ACE"

Cyber Incident Response means the process of exchanging necessary information on a cybersecurity incident with individuals or organizations responsible for conducting or coordinating remediation to address the cybersecurity incident.

Vulnerability disclosure means the process of identifying, reporting, or communicating a vulnerability to, or analyzing a vulnerability with, individuals or organizations responsible for conducting or coordinating remediation for the purpose of resolving the vulnerability.

Cyber Tools – Guidance

Revised FAQs to address some of the comments

Decision Tree on BIS website

Additional clarifications

Questions?