

Overview of the June 25, 2010 Encryption Control Rewrite (75 FR 36482)

George R. Tuttle, III
George R. Tuttle Law Offices
One Embarcadero Center, Suite 730, San Francisco
Phone (415) 986-8780
E-mail: Geo@tuttlelaw.com

The information in this article is general in nature and is not intended to constitute legal advice or to create an attorney-client relationship with respect to any event or occurrence, and may not be considered as such. You should contact your attorney to obtain advice with respect to any particular issue or question.

What you will Learn

- Changes to:
 - Category 5 (Part 2) - Information Security
 - ECCN 5A002 & 5D002
 - Overview of Decontrolled Encryption Products
 - Revisions to License Exception ENC
 - New Encryption registration requirements
 - New Self Classification Annual Reporting
 - Grandfathering clause for previous CCATS decisions

Part 772 “Definition of terms”

- Cat. 5, Part II-- “*Information security*”
 - Broadly defined as:
 - The means and functions for ensuring the accessibility, confidentiality or integrity of information or communications
 - Excludes “means and functions intended to safeguard against malfunctions”
 - includes “cryptography”, “cryptanalysis”, and features for protection against compromising emanations (TEMPEST) and computer security.

“Cryptanalysis”

- *the analysis of a cryptographic system or its inputs and outputs to derive confidential variables or sensitive data, including clear text. (ISO 7498-2-1988 (E), paragraph 3.3.18)*
- *Functions specially designed and limited to protect against malicious computer damage or unauthorized system intrusion (e.g., viruses, worms and Trojan horses) are not construed to be cryptanalytic functions.*

Part 772 “Definition of terms”

- “Cryptography”
 - The means and methods for transformation of data in order to hide its information content, prevent its undetected modification or prevent its unauthorized use
 - “Cryptography” is limited to the transformation of information using one or more “secret parameters” (e.g., crypto variables) and/or associated key management.
 - “Cryptography” does not include “fixed” data compression or coding techniques. 5A002.a.1 Technical note 3.

740.17(b)(2) Note

- Commodities, software, and components (dongles and keys) that allow the end-user to:
 - activate or enable cryptographic functionality in encryption products which would otherwise remain disabled
 - controlled according to the functionality of the activated encryption product.
 - Disabled product is generally 5D992

General Notes to Category 5 (Part 2) - Exclusions

- Notes 2, 3, and 4 are exclusion notes
 - Note 2. Personal use / *tools of trade*, *License Exceptions TMP or BAG*
 - Note 3. Mass Market cryptographic note resulting in 5X992 classifications
 - Note 4. Ancillary encryption products that have been removed from C5 P2.

General Notes to Category 5 (Part 2) – Note 4

- Excludes items that incorporate or use “cryptography” from Category 5, Part 2 if the **primary function** of the item is not:
 - “information security,”
 - computing, communications,
 - storing information,
 - networking, and
 - the cryptographic functionality is limited to supporting the primary function or set of functions if the item.

General Notes to Category 5 (Part 2) -- Note 4

- The primary function is the “obvious or main purpose” of the item
 - It is the function which is not there to support other functions.
 - The primary function or set of functions is **not** any of the following:
 - “Information security”
 - A computer, including operating systems, parts and components;
 - Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management)
 - Networking (includes operation, administration, management and provisioning);

General Notes to Category 5 (Part 2) -- Note 4

- The “communications” and “information storage” primary function does **not** include items that:
 - support entertainment, mass commercial broadcasts, digital rights management or medical records management.
- Products that are excluded by Note 4 to Category 5 (Part 2) should be evaluated under other categories of the CCL to determine if any other controls apply.

“Ancillary cryptography”

- Examples of items that are excluded from Category 5, Part 2 by **Note 4**:
 - Piracy and theft prevention for software or music; games and gaming;
 - household utilities and appliances;
 - printing, reproduction, imaging and video recording or playback (not videoconferencing);
 - business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery);

“Ancillary cryptography”

- “Ancillary cryptography”, cont.
 - industrial, manufacturing or mechanical systems (e.g., robotics, heavy equipment, facilities systems such as fire alarm, HVAC);
 - automotive, aviation, and other transportation systems;
 - LCD TV, Blu-ray/DVD, video on demand (VoD), cinema, digital video recorders (DVRs)/personal video recorders (PVRs);
 - on-line media guides, commercial content integrity and protection, HDMI and other component interfaces;
 - medical/clinical—including diagnostic applications, patient scheduling, and medical data records confidentiality;

“Ancillary cryptography”

- “Ancillary cryptography”, cont.
 - academic instruction and testing/on-line training—tools and software;
 - applied geosciences—mining/ drilling, atmospheric sampling/weather monitoring, mapping/surveying, dams/ hydrology; scientific visualization/ simulation/co-simulation (excluding such tools for computing, networking, or cryptanalysis);
 - data synthesis tools for social, economic, and political sciences (e.g., economic, population, global climate change, public opinion polling, forecasting and modeling);
 - software and hardware design IP protection; and
 - computer aided design (CAD) software and other drafting tools

5A002 “Information security” systems, equipment and components-- Exclusions

- *5A002 does not control any of the following:*
 - (a) Smart cards and smart card ‘readers/writers
 - (b) products covered by **Note 4** in Category 5 - Part 2
 - (d) Cryptographic equipment specially designed and limited for banking use or money transactions
 - (e) Portable or mobile radio-telephones for civil use (e.g., for use with commercial civil cellular radio communication systems) that are **not** capable of transmitting encrypted data

5A002 “Information security” systems, equipment and components-- Exclusions

- (f) Cordless telephone equipment not capable of end-to-end encryption where the maximum effective range is less than 400 meters according to the manufacturer's specifications
 - (g) Portable or mobile radio-telephones and similar client wireless devices for civil use, that implement **only** published or commercial cryptographic standards
 - (i) Wireless “personal area network” equipment that implement **only** published or commercial cryptographic standards and where the cryptographic capability is limited to a nominal operating range not exceeding 30 meters.
- These items are instead controlled under 5A992

5A002 “Information security” systems, equipment and components-- Exclusions

- 5A002.a.1-- *Technical Note: Authentication and digital signature functions are not controlled by 5A002 or 5D002*
 - *Authentication and digital signature functions including associated key management function.*
 - Authentication includes all aspects of access control where there is no encryption of files or text except as directly related to the protection of passwords, Personal Identification Numbers (PINs) or similar data to prevent unauthorized access.

5A002 “Information security” systems, equipment and components

- Systems, equipment, application specific “electronic assemblies”, modules and integrated circuits for “information security”, as follows, and components therefor specially designed for “information security”:
- Designed or modified to use “cryptography” employing digital techniques performing any cryptographic function **other than** authentication or digital signature and having any of the following:
 - a.1.a. A “symmetric algorithm” employing a key length in excess of 56-bits;

5A002 “Information security” systems, equipment and components

- a.1.b. An “asymmetric algorithm” where the security of the algorithm is based on any of the following:
 - a.1.b.1. Factorization of integers in excess of 512 bits (e.g., RSA);
 - a.1.b.2. Computation of discrete logarithms in a multiplicative group of a finite field of size greater than 512 bits (e.g., Diffie-Hellman over Z/pZ); or
 - a.1.b.3. Discrete logarithms in a group other than mentioned in 5A002.a.1.b.2 in excess of 112 bits (e.g., Diffie-Hellman over an elliptic curve);
- a.2. Designed or modified to perform cryptanalytic functions;
- Products classified under 5A002 or 5D002 may be eligible for License exception ENC.

Mass Market Encryption

- Mass-market encryption defined in **Note 3**
 - *ECCNs 5A002 and 5D002 do not control items that are:*
 - **a.** *Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:*
 - 1. *Over-the-counter transactions;*
 - 2. *Mail order transactions;*
 - 3. *Electronic transactions; or*
 - 4. *Telephone call transactions;*
 - **b.** *The cryptographic functionality cannot be easily changed by the user;*

Examples of Mass Market Encryption Products

- Mass market encryption products include, but are not limited to:
 - general purpose operating systems and desktop applications (e.g., e-mail, browsers, games, word processing, database, financial applications or utilities) designed for use with computers classified as ECCN 4A994 or designated as EAR99, laptops, or hand-held devices;
 - commodities and software for client Internet appliances and client wireless LAN devices;
 - home use networking commodities and software (e.g., personal firewalls, cable modems for personal computers, and consumer set top boxes);
 - Portable or mobile civil telecommunications commodities and software (e.g., personal data assistants (PDAs), radios, or cellular products).

§742.15(b) -- Encryption Registration

- Most Mass market encryption commodities and software is released from “EI” and “NS” controls after:
 - submitting an encryption registration in accord with § 742.15(b) of the EAR (SNAP-R), and
 - Receiving an Encryption Registration Number (ERN)
 - commodities or software are then classified under ECCNs 5A992 and 5D992, and no longer subject to “EI” and “NS” controls.

§742.15(b) -- Encryption Registration

- Mass-Market Rules
 - **Low strength mass market items:**
 - Mass market commodities and software with symmetric key lengths less than or equal to 64 bits for symmetric algorithms, or
 - if there are no symmetric algorithms then 768 bits for asymmetric algorithms or
 - 128 bits for elliptic curve algorithms
 - are not controlled under 5A002 or 5D002 and may be self-classified as 5A992 or 5D992.
 - mass market items with short range wireless functionality described by Section 742.15(b)(4) (< 100 meters)
 - may be exported and reexported under the symbol NLR (No License Required) without
 - mass market classification request,
 - encryption registration OR self-classification reporting requirements.

§742.15(b) -- Encryption Registration

- **Higher strength mass market items not identified in Section 742.15(b)(3):**
 - Mass market commodities and software, except certain mass market items identified in Section 742.15(b)(3), with
 - key lengths greater than or equal to 64 bits for symmetric algorithms, or,
 - if no symmetric algorithms, then 768 bits for asymmetric algorithms, or 128 bits for elliptic curve algorithms
 - no longer require an encryption review prior to export or reexport.
 - Such mass market items are classified as 5A002 or 5D002 but may be self-classified as 5A992 or 5D992 after encryption registration under the symbol NLR (No License Required).
 - (b)(3) = chipsets, development kits, etc., non-standard enc. software require submission of classification request.

§742.15(b) --Mass Market Encryption

- Note:
 - Encryption items that are described in §§ 740.17(b)(2) or (b)(3)(iii) of the EAR do not qualify for mass market treatment.
 - High-end network infrastructure products (b)(2)
 - Other than high-end infrastructure (components, toolkits) products (b)(3)
 - Does not authorize export or reexport to any country listed in Country Group E:1 in Supplement No. 1 to part 740.

Self-Classification of Mass Market

- Mass Market products that require a classification request to BIS (742.15(b)(3)):
 - Chips, chipsets, electronic assemblies and field programmable logic devices;
 - Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);
 - Application-specific hardware or software development kits implementing cryptography.
 - Mass market encryption products that provide or perform “non-standard cryptography”

Self-Classification of Mass Market

- All other (non-742.15(b)(3) products) Mass-Market products may be self-classified by exporter / producer:
 - No BIS one-time review required
 - May use ECCNs 5A992 or 5D992 following submission of encryption registration and receipt of encryption registration number.
 - Self-classified mass-market products have an annual reporting requirement (742.15(c))

Exclusions From Mass Market Classification, Registration and Reporting Requirements

- When an exporter or reexporter relies on a producer's:
 - self-classification (pursuant to the producer's encryption registration) or
 - CCATS for a mass market encryption item,
- not required to submit an encryption registration, classification request or self-classification report.

Exclusions From Mass Market Classification, Registration and Reporting Requirements

- Short range wireless products with encryption functions (e.g., with a nominal operating range not exceeding 100 meters)
- Foreign products developed with or incorporating U.S. origin encryption source code, components or toolkits that are subject to the EAR, **provided** that the U.S. origin encryption items have previously been classified or registered and authorized by BIS and the cryptographic functionality has not been changed.

Mass market encryption registration -- Submission requirements

- Must complete BIS-748P Multipurpose Application Form (SNAP-R).
- Use instructions from 748(r) to complete
- Must include information from Supplement 5 to Part 742
- Registration is required only once unless the answers to Suppl 5 changes.
- Suppl. 6 information for (b)(1) articles on an as-needed basis upon request by BIS

Suppl. 5

SUPPLEMENT NO. 5 TO PART 742 - ENCRYPTION REGISTRATION

Certain classification requests and self-classification reports for encryption items must be supported by an encryption registration, i.e., the information as described in this Supplement, submitted as a support documentation attachment to an application in accordance with the procedures described in §§ 740.17(b), 740.17(d), 742.15(b), 748.1, 748.3 and Supplement No. 2 to part 748 of the EAR.

(1) Point of Contact Information

- (a) Contact Person
- (b) Telephone Number
- (c) Fax Number
- (d) E-mail address
- (e) Mailing Address

(2) Company Overview (approximately 100 words).

(3) Identify which of the following categories apply to your company's technology/families of products:

- (a) Wireless
 - (i) 3G cellular
 - (ii) 4G cellular/WiMax/LTE
 - (iii) Short-range wireless / WLAN
 - (iv) Satellite
 - (v) Radios
 - (vi) Mobile communications, n.e.s.
- (b) Mobile applications
- (c) Computing platforms
- (d) Multimedia over IP
- (e) Trusted computing
- (f) Network infrastructure
- (g) Link layer encryption
- (h) Smartcards or other identity management
- (i) Computer or network forensics
- (j) Software
 - (i) Operating systems
 - (ii) Applications

- (k) Toolkits / ASICs / components
- (l) Information security including secure storage
- (m) Gaming
- (n) Cryptanalytic tools
- (o) "Open cryptographic interface" (or other support for user-supplied or non-standard cryptography)
- (p) Other (identify any not listed above)
- (q) Not Applicable (Not a producer of encryption or information technology items)

(4) Describe whether the products incorporate or use proprietary, unpublished or non-standard cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body. (If unsure, please explain)

(5) Will your company be exporting "encryption source code"?

(6) Do the products incorporate encryption components produced or furnished by non-U.S. sources or vendors? (If unsure, please explain)

(7) With respect to your company's encryption products, are any of them manufactured outside the United States? If yes, provide manufacturing locations. (Insert "not applicable", if you are not the principal producer of encryption products)

Annual Self-classification Reporting

- 742.15(c) -- Self-classification Reporting requirements
- **When to report**– encryption commodities, software and components exported or reexported during a calendar year (January 1 through December 31)
- No later than February 1 of the following year

Annual Self-classification Reporting

- **How to report**

- Encryption self-classification reports must be sent to BIS and the ENC Encryption Request Coordinator via e-mail or regular mail.
- Specify the export timeframe
- identify points of contact to whom questions or other inquiries pertaining to the report should be directed.

Annual Self-classification Reporting

- **Submissions via e-mail**

- Submit encryption self-classification report electronically to BIS at crypt-supp8@bis.doc.gov and to the ENC Encryption Request Coordinator at enc@nsa.gov, as an attachment to an e-mail.
- Identify your e-mail with subject “Self-classification report for ERN R#####”
- Use most recent ERN in the subject line (so as to correspond your encryption self-classification report to your most recent encryption registration ERN).

Annual Self-classification Reporting

- **Information to report**
- Identifies products exported not individual shipments
- Encryption self-classification report must include:
 - The information described in paragraph (a) of Supplement No. 8 for each applicable article.
 - If no information has changed since the previously submitted report, you must either send an e-mail stating that nothing has changed since the previous report or submit a copy of the previously submitted report.

Supplement No. 8

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 manufacturer of the item. If there are multiple manufacturers for the item but none is clearly primary, either enter the name of one of the manufacturers or else enter 'MULTIPLE'. If necessary, enter 'NONE' or 'N/A'.

(4) Export Control Classification Number (ECCN), selected from one of the following:

- (i) 5A002
- (ii) 5B002
- (iii) 5D002
- (iv) 5A992
- (v) 5D992

(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
 - (xviii) key storage
 - (xix) link encryption
 - (xx) local area networking (LAN)
 - (xxi) metropolitan area networking (MAN)
 - (xxii) modem
 - (xxiii) network convergence or infrastructure
- n.e.s.
- (xxiv) network forensics
 - (xxv) network intelligence
 - (xxvi) network or systems management
- (OAM / OAM&P)
- (xxvii) network security monitoring
 - (xxviii) network vulnerability and penetration
- testing
- (xxix) operating system
 - (xxx) optical networking
 - (xxxii) radio communications

Suppl. 8

- (xxxii) router
- (xxxiii) satellite communications
- (xxxiv) short-range wireless n.e.s.
- (xxxv) storage area networking (SAN)
- (xxxvi) 3G / 4G / LTE / WiMAX
- (xxxvii) trusted computing
- (xxxviii) videoconferencing
- (xxxix) virtual private networking (VPN)
- (xl) voice communications n.e.s.
- (xli) voice over Internet protocol (VoIP)
- (xlii) wide area networking (WAN)
- (xliii) wireless local area networking (WLAN)
- (xliv) wireless personal area networking (WPAN)
- (xlv) commodities n.e.s.
- (xlvi) components n.e.s.
- (xlvii) software n.e.s.
- (xlviii) test equipment n.e.s.
- (xlix) OTHER

(b) File format requirements.

(1) The information described in paragraph (a) of this supplement must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv), only. No file formats other than .csv will be accepted, as your encryption self-classification report must be directly convertible to tabular or spreadsheet format, where each row (and all entries within a row) properly correspond to the appropriate encryption item.

Note to paragraph (b)(1): *An encryption self-classification report data table created and stored in spreadsheet format (e.g., file extension .xls, .numbers, .qpw, .wb*, .wrk, and .wks) can be converted and saved into a comma delimited file format directly from the spreadsheet program. This .csv file is then ready for submission.*

(2) Each line of your encryption self-classification report (.csv file) must consist of six entries as further described in this supplement.

(3) The first line of the .csv file must consist of

the following six entries (i.e., match the following) without alteration or variation: PRODUCT NAME, MODEL NUMBER, MANUFACTURER, ECCN, AUTHORIZATION TYPE, ITEM TYPE

Note to paragraph (b)(3): *These first six entries (i.e., first line) of a encryption self-classification report in .csv format correspond to the six column headers (i.e., first row) of a spreadsheet data file.*

(4) Each subsequent line of the .csv file must correspond to a single encryption item (or a distinguished series of products) as described in paragraph (c) of this supplement.

(5) Each line must consist of six entries as described in paragraph (a)(1), (a)(2), (a)(3), (a)(4), (a)(5), and (a)(6) of this supplement. No entries may be left blank. Each entry must be separated by a comma (.). Certain additional instructions are as follows:

(i) Line entries (a)(1) ('PRODUCT NAME') and (a)(4) ('ECCN') must be completed with relevant information.

(ii) For entries (a)(2) ('MODEL NUMBER') and (a)(3) ('MANUFACTURER'), if these entries do not apply to your item or situation you may enter 'NONE' or 'N/A'.

(iii) For entries (a)(5) ('AUTHORIZATION TYPE'), if none of the provided choices apply to your situation, you may enter 'OTHER'.

(6) Because of .csv file format requirements, the only permitted use of a comma is as the necessary separator between line entries. You may not use a comma for any other reason in your encryption self-classification report.

(c) Other instructions

(1) The information provided in accordance with this supplement and §§ 740.17(b)(1), 742.15(b)(1) and 742.15(c) of the EAR must

Supplement 8– Annual Reporting

Control Policy—CCL Based Controls

Supplement No. 8 to Part 742–page 3

identify product offerings as they are typically distinguished in inventory, catalogs, marketing brochures and other promotional materials.

(2) For families of products where all the information described in paragraph (a) of this supplement is identical except for the model / series / part number (entry (a)(2)), you may list and describe these products with a single line in your .csv file using an appropriate model / series / part number identifier (e.g., ‘300’ or ‘3xx’) for entry (a)(2), provided each line in your .csv file corresponds to a single product series (or product type) within an overall product family.

(3) For example, if Company A produces, markets and sells both a ‘100’ (‘1xx’) and a ‘300’ (‘3xx’) series of product, in its encryption self-classification report (.csv file) Company A must list the ‘100’ product series in one line (with entry (a)(2) completed as ‘100’ or ‘1xx’) and the ‘300’ product series in another line (with entry (a)(2) completed as ‘300’ or ‘3xx’), even if the other required information is common to all products in the ‘100’ and ‘300’ series.

Annual Self-classification Reporting

- ***File format requirements***

- The information described in paragraph (a) of this supplement must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv), only.
- No file formats other than .csv will be accepted, as your encryption self-classification report must be directly convertible to tabular or spreadsheet format, where each row (and all entries within a row) properly correspond to the appropriate encryption item.
- **Note to paragraph (b)(1):** *An encryption self-classification report data table created and stored in spreadsheet format (e.g., file extension .xls, .numbers, .qpw, .wb*, .wrk, and .wks) can be converted and saved into a comma delimited file format directly from the spreadsheet program.*

Self-Classification Report

	-1	-2	-3	-4	-5	-6
	Product Name	Model / series / part number	Primary manufacturer	ECCN	authorization type identifier	Item type descriptor
Item						

Mass market encryption Classification -- Submission requirements

- Applies to articles defined by 742.15(b)(3)
- Prior to application Encryption Registration is required.
- Requires submission of Supplement 6, Part 742.
- Once application is accepted, may export under ENC as ECCN 5A002 or 5D002 to end users located or Headquartered in Suppl. 3, part 740 while application is pending
- 30 days after submission may use 5A992 or 5D992

Suppl 6

SUPPLEMENT NO. 6 – TECHNICAL QUESTIONNAIRE FOR ENCRYPTION ITEMS

(a) For all encryption items:

(1) State the name(s) of each product being submitted for classification or other consideration (as a result of a request by BIS) and provide a brief non technical description of the type of product (e.g., routers, disk drives, cell phones, and chips) being submitted, and provide brochures, data sheets, technical specifications or other information that describe the item(s).

(2) Indicate whether there have been any prior classifications or registrations of the product(s), if they are applicable to the current submission. For products with minor changes in encryption functionality, you must include a cover sheet with complete reference to the previous review (Commodity Classification Automated Tracking System (CCATS) number, Encryption Registration Number (ERN), Export Control Classification Number (ECCN), authorization paragraph) along with a clear description of the changes.

(3) Describe how encryption is used in the product and the categories of encrypted data (e.g., stored data, communications, management data, and internal data).

(4) For 'mass market' encryption products, describe specifically to whom and how the product is being marketed and state how this method of marketing and other relevant information (e.g., cost of product and volume of sales) are described by the Cryptography Note (Note 3 to Category 5, Part 2).

(5) Is any "encryption source code" being provided (shipped or bundled) as part of this offering? If yes, is this source code publicly available source code, unchanged from the code obtained from an open source web site, or is it proprietary "encryption source code?"

(b) For classification requests and other submissions for an encryption commodity or software, provide the following information:

(1) Description of all the symmetric and asymmetric encryption algorithms and key lengths and how the algorithms are used, including relevant parameters, inputs and settings. Specify which encryption modes are supported (e.g., cipher feedback mode or cipher block chaining mode).

(2) State the key management algorithms, including modulus sizes that are supported.

(3) For products with proprietary algorithms, include a textual description and the source code of the algorithm.

(4) Describe the pre-processing methods (e.g., data compression or data interleaving) that are applied to the plaintext data prior to encryption.

(5) Describe the post-processing methods (e.g., packetization, encapsulation) that are applied to the cipher text data after encryption.

(6) State all communication protocols (e.g., X.25, Telnet, TCP, IEEE 802.11, IEEE 802.16, SIP ...) and cryptographic protocols and methods (e.g., SSL, TLS, SSH, IPSEC, IKE, SRTP, ECC, MD5, SHA, X.509, PKCS standards...) that are supported and describe how they are used.

(7) Describe the encryption-related Application Programming Interfaces (APIs) that are implemented and/or supported. Explain which interfaces are for internal (private) and/or external (public) use.

(8) Describe the cryptographic functionality that is provided by third-party hardware or software encryption components (if any). Identify the manufacturers of the hardware or software

components, including specific part numbers and version information as needed to describe the product. Describe whether the encryption software components (if any) are statically or dynamically linked.

(9) For commodities or software using Java byte code, describe the techniques (including obfuscation, private access modifiers or final classes) that are used to protect against decompilation and misuse.

(10) State how the product is written to preclude user modification of the encryption algorithms, key management and key space.

(11) Describe whether the product meets any of the §740.17(b)(2) criteria. Provide specific data for each of the parameters listed, as applicable (e.g., maximum aggregate encrypted user data throughput, maximum number of concurrent encrypted channels, and operating range for wireless products).

(12) For products which incorporate an “open cryptographic interface” as defined in part 772 of the EAR, describe the cryptographic interface.

(c) For classification requests for hardware or software “encryption components” other than source code (i.e., chips, toolkits, executable or linkable modules intended for use in or production of another encryption item) provide the following additional information:

(1) Reference the application for which the components are used in, if known;

(2) State if there is a general programming interface to the component;

(3) State whether the component is constrained by function; *and*

(4) Identify the encryption component and include the name of the manufacturer, component model number or other identifier.

(d) For classification requests for “encryption source code” provide the following information:

(1) If applicable, reference the executable (object code) product that was previously classified by BIS or included in an encryption registration to BIS;

(2) Include whether the source code has been modified, and the technical details on how the source code was modified; *and*

(3) *Upon request*, include a copy of the sections of the source code that contain the encryption algorithm, key management routines and their related calls.

License exception ENC

- License Exception ENC authorizes export and reexport of:
 - systems, equipment, commodities and components therefor that are classified under ECCNs 5A002.a.1, a.2, a.5, a.6 or a.9,
 - systems, equipment and components therefor classified under ECCN 5B002, and
 - equivalent or related software and technology classified under ECCNs 5D002 or 5E002.

License exception ENC

- License Exception ENC authorizes exports and reexports to
 - 'private sector end-users' wherever located that are headquartered in a country listed in Supplement No. 3 to part 740 for:
 - internal “development” or “production” of new products by those end-users.
 - Items classified under ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9, ECCN 5B002, and equivalent or related software and technology classified under ECCNs 5D002 or 5E002

License exception ENC

- A *'private sector end-user'* is:
 - (1) An individual who is not acting on behalf of any foreign government; or
 - (2) A commercial firm (including its subsidiary and parent firms, and other subsidiaries of the same parent) that is not wholly owned by, or otherwise controlled by or acting on behalf of, any foreign government.

License exception ENC

- Exports and reexports to “U.S. Subsidiaries”
 - ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9,
 - systems, equipment, and components therefor classified under ECCN 5B002,
 - equivalent or related software and technology classified under ECCNs 5D002 or 5E002

License exception ENC

- Exports and reexports to “U.S. Subsidiaries”
 - Applies to any “U.S. subsidiary,” wherever located
 - No submission of an encryption registration, classification request, self-classification report or sales report to BIS.
 - Authorizes export or reexport to foreign nationals who are employees, contractors or interns of a U.S. company or its subsidiaries if the items are for internal company use,
 - includes “development” or “production” of new products, without prior review by the U.S. Government

License exception ENC

- Encryption commodities, software or components described in (b)(2) or (b)(3) of 740.17 require submission of an ENC classification request.
- Encryption commodities, software or components classified under
 - ECCNs 5A002.a.1, .a.2, .a.5, .a.6, or .a.9,
 - ECCN 5B002, and
 - equivalent or related software classified under ECCN 5D002,
- And **not** described in (b)(2) or (b)(3) of 740.17 may be immediately exported, subject to:
 - Encryption Registration process and ERN issuance
 - Subject to Annual Self-classification Report

License exception ENC– (b)(2)

- Encryption commodities, software or components described in (b)(2) of 740.17
 - Network infrastructure software and commodities and components thereof providing secure Wide Area Network (WAN), Metropolitan Area Network (MAN), Virtual Private Network (VPN), satellite, digital packet telephony/media (voice, video, data) over internet protocol, cellular or trunked communications meeting any of the following with key lengths exceeding 80-bits for symmetric algorithms:

License exception ENC– (b)(2)

- Network infrastructure software and commodities
- key lengths exceeding 80-bits for symmetric algorithms:
 - **(1)** Aggregate encrypted WAN, MAN, VPN or backhaul throughput (including communications through wireless network elements such as gateways, mobile switches, and controllers) greater than 90 Mbps;

License exception ENC– (b)(2)

- **(2)** Wire (line), cable or fiber optic WAN, MAN or VPN single channel input data rate exceeding 154 Mbps;
- **(3)** Transmission over satellite at data rates exceeding 10 Mbps
- **(4)** Media (voice/video/data) encryption or centralized key management supporting more than 250 concurrent encrypted data channels, or encrypted signaling to more than 1,000 endpoints, for digital packet telephony / media (voice/video/data) over internet protocol communications;

License exception ENC—(b)(2)

- **(5)** Air interface coverage (e.g., through base stations, access points to mesh networks, and bridges) exceeding 1,000 meters, where any of the following applies:
 - **(i)** Maximum transmission data rates exceeding 10 Mbps (at operating ranges beyond 1,000 meters);
 - **(ii)** Maximum number of concurrent full-duplex voice channels exceeding 30; *or*
 - **(iii)** Substantial support is required for installation or use;

License exception ENC– (b)(2)

- **(B)** Encryption source code that would not be eligible for export or reexport under License Exception TSU because it is not publicly available as that term is used in § 740.13(e)(1) of the EAR;
- **(C)** Encryption software, commodities and components, that have any of the following:
 - **(1)** Been designed, modified, adapted or customized for “government end-user(s)”;
 - **(2)** Cryptographic functionality that has been modified or customized to customer specification; *or*
 - **(3)** Cryptographic functionality or “encryption component” (except encryption software that would be considered publicly available, as that term is used in § 740.13(e)(1) of the EAR) that is user-accessible and can be easily changed by the user;

License exception ENC– (b)(2)

- **(D)** Encryption commodities and software that provide functions necessary for quantum cryptography, as defined in ECCN 5A002 of the Commerce Control List;
- **(E)** Encryption commodities and software that have been modified or customized for computers classified under ECCN 4A003;
- **(F)** Encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks
- **(G)** Public safety / first responder radio

License exception ENC– (b)(2)

- **(ii) Cryptanalytic commodities and software.**
 - Commodities and software classified as “cryptanalytic items” to non “government end users” located or headquartered in countries not listed in Supplement No. 3;
- **(iii) “Open cryptographic interface” items**
 - Items that provide an “open cryptographic interface”, to any end-user located or headquartered in a country listed in Supplement No. 3 to this part.
- **(iv) Specific encryption technology**
 - “non-standard cryptography”
 - Other Encryption technology

License exception ENC– (b)(2)

- Requires:
 - Encryption Registration (Submit Supp. 5, Part 742 in SNAP) ERN
 - Classification Req. w/ 30 day wait (Submit Supp.6, Part 742 in SNAP)
 - Semi-Annual Reporting (see 740.17 (e))
- Immediate export to Supp. 3
- 30 day wait outside Supp. 3
- No Gov't outside Supp. 3
- -Cryptanalytic: No Gov't;
- non-stand/cryptanalytic tech and OCI: Supp. 3 only;

License exception ENC– (b)(3)

- (b)(3) list items require the submission of a classification request before being eligible for export under license exception ENC:
 - **(A)** Chips, chipsets, electronic assemblies and field programmable logic devices;
 - **(B)** Cryptographic libraries, modules, development kits and toolkits, including for operating systems and cryptographic service providers (CSPs);
 - **(C)** Application-specific hardware or software development kits implementing cryptography.

License exception ENC– (b)(3)

- (ii) Encryption commodities, software and components not described by paragraph (b)(2) of this section, that provide or perform “non-standard cryptography” as defined in part 772 of the EAR.
- (iii) Encryption commodities and software not described by paragraph (b)(2) of this section, that provide or perform vulnerability analysis, network forensics, or computer forensics functions
- (iv) Cryptographic enabling commodities and software where the product or cryptographic functionality is not otherwise described in paragraphs (b)(2) or (b)(3)(i).

License exception ENC– (b)(3)

- Requires:
 - Encryption Registration (Submit Supp. 5, Part 742 in SNAP) and wait for ERN.
 - Classification Req. (Submit Supp.6, Part 742 in SNAP) w/ 30 day wait
 - Semi-Annual Report for b.3.iii product only (see 740.17(e))
- Immediate export to Supplement No. 3 countries.
- 30 day wait outside Supplement No. 3 countries.

Semi-Annual Reporting (740.17(e))

- Items described under paragraphs (b)(2) and (b)(3)(iii)
- Required for exports to all destinations other than Canada
- For reexports from Canada
- Information required
 - CCATS number
 - name of the item(s)
 - the name and address of the distributor or reseller, the item and the quantity, by the
 - The end user's name and address if collected
 - **Direct Sales:** the name and address of the recipient, the item, and the quantity exported

Exclusions from reporting requirement.

- Reporting is not required for the following items and transactions:
 - Encryption commodities or software with a symmetric key length not exceeding 64 bits;
 - Encryption items exported via free and anonymous download;
 - Foreign products developed by bundling or compiling of source code
 - Key length increases

Grandfathering Issues

- General Rule
 - No need to file encryption registration or a new classification request for CCATS issued prior to June 24, 2010.
 - Must continue to provide semiannual reporting for items classified under 740.17(b)(2) and (b)(3)(iii)
- Exceptions
 - When encryption functionality changes
 - Products that are now classified under (b)(2) that were not previously

Approaching Encryption Issues

- Does the product or software have encryption => 5A002.a.1 para?
- Is the product exempt from C5 P2 by note 4?
- Is the cryptographic function limited to authentication or digital signature?
- Is the product mass-market? (Note 3 and 742.15)
 - Can the product be self-classified? (not (b)(2) product)
 - Requires annual self-class report
- Is the item ENC eligible?
 - Can the product be self-classified? (not (b)(2) or (b)(3) product)
 - Requires annual self-class report
 - (b)(2) or (b)(3) products require annual sales report

Mass-Market Chart

742.15 Sub¶	Item Description	ECCN	End Users	Submission Requirements
(b)(1)	Items that meet Note 3 of Category 5, Part 2 (>64/768/128 bit) and are not items described in 742.15 (b)(3) or (b)(4).	5A992.c 5D992.c	All except E:1	1. Encryption Registration (Submit Supp. 5, Part 742 in SNAP) ERN 2. Annual Self-Classification Report (Submit Supp. 8, Part 742 in email)
(b)(3)	Meet Note 3, and are: (i) Encryption components: chips, electronic assemblies, crypto libraries, toolkit, development kits; or (ii) Non-standard crypto items	5A992.c 5D992.c	All except E:1	1. Encryption Registration (Submit Supp. 5, Part 742 in SNAP) ERN 2. Classification Req. w/ 30 day wait (Submit Supp.6, Part 742 in SNAP) CCATS
(b)(4)	Meet Note 3, and are short-range wireless	5A992.c 5D992.c	All except E:1	None

LICENSE EXCEPTION ENC (740.17)

740.17 Sub¶	Item Description or Purpose of Export	ECCN	End User Authorized (outside <u>E:1</u>)	Submission Requirements
(a)(1)	Development/Production only	5A002.a.1, a.2, .a.5, a.6, a.9, 5B002, 5D002, 5E002	Private end user in or HQ'ed in <u>Supplement No. 3</u> countries	None*
(a)(2)	Any internal purpose	5A002.a.1, a.2, .a.5, a.6, a.9, 5B002, 5D002, 5E002	U.S. Subs (employees, interns, contractors)	None*
(b)(1)	All encryption items except items described in (b)(2) and (b)(3)	5A002.a.1, a.2, .a.5, a.6, a.9, 5B002, 5D002	All except <u>E:1</u> countries	1. Encryption Registration (Submit <u>Supp. 5, Part 742</u> in SNAP) ERN 2. Annual Self-Classification Report (Submit <u>Supp. 8, Part 742</u> in email)
(b)(2)	Network infrastructure, source code, designed for gov't, custom crypto, modifiable crypto, quantum crypto, penetration testing, public safety radio, cryptanalytic, non-standard tech, OCI, encryption technology	5A002.a.1, a.2, .a.5, a.6, a.9, 5D002, 5E002	- Immediate export to <u>Supp. 3</u> - 30 day wait outside <u>Supp. 3</u> - No Gov't outside <u>Supp. 3</u> - Cryptanalytic: No Gov't; - non-stand/cryptanalytic tech and OCI: <u>Supp. 3</u> only; - 5E002: no <u>D:1</u> countries (unless HQ'ed in <u>Supp. 3</u>)	1. Encryption Registration (Submit <u>Supp. 5, Part 742</u> in SNAP) ERN 2. Classification Req. w/ 30 day wait (Submit <u>Supp.6, Part 742</u> in SNAP) 3. Semi-Annual Report by email (see 740.17 (e))
(b)(3)	(i) Encryption components: chips, electronic assemblies, crypto libraries, toolkit, dev kits (ii) Non-standard crypto items, (iii) Digital forensics	5A002.a.1, a.2, .a.5, a.6, a.9, 5D002	- Immediate export to <u>Supplement No. 3</u> countries. - 30 day wait outside <u>Supplement No. 3</u> countries	1. Encryption Registration (Submit <u>Supp. 5, Part 742</u> in SNAP) ERN 2. Classification Req. w/ 30 day wait (Submit <u>Supp.6, Part 742</u> in SNAP) 3. Semi-Annual Report for b.3.iii only, by email (see 740.17(e))
(b)(4)	(i) Short-range Wireless (ii) Foreign dev with US enc parts	5A002.a.1, a.2, .a.5, a.6, a.9, 5D002	All except <u>E:1</u> countries	None

*Developed products are subject to the EAR