(i) *North Korea.* Applications for military end-users or for military end-uses, or for nuclear end-users or nuclear end-uses, in North Korea of such equipment will generally be denied. Applications for non-military end-users or for non-military end-uses, or for non-nuclear end-users or non-nuclear end-uses, in North Korea will be considered on a case-by-case basis.

(ii) [Reserved]

(46) *Concealed object detection equipment described in ECCN 2A984.*

(i) *Syria.* Applications for all end-users in Syria of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan.* Applications for all end-users in Sudan of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea.* Applications for all end-users in North Korea of these commodities will generally be denied. Contract sanctity date: March 19, 2010.

(47) *''Software'' described in ECCN 2D984 ''required'' for the ''development'', ''production'' or ''use'' of concealed object detection equipment controlled by 2A984.*

(i) *Syria.* Applications for all end-users in Syria of these software will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan.* Applications for all end-users in Sudan of these software will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea.* Applications for all end-users in North Korea of these software will generally be denied. Contract sanctity date: March 19, 2010.

(48) *''Technology'' described in ECCN 2E984 ''required'' for the ''development'', ''production'' or ''use'' of concealed object detection equipment controlled by 2A984, or the ''development'' of ''software'' controlled by 2D984.*

(i) *Syria.* Applications for all end-users in Syria of these items will generally be denied. Contract sanctity date: March 19, 2010.

(ii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied. Contract sanctity date: March 19, 2010.

(iii) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: March 19, 2010.

[69 FR 23630, Apr. 29, 2004, as amended at 69 FR 46076, July 30, 2004; 70 FR 14391, Mar. 22, 2005; 71 FR 20885, Apr. 24, 2006; 71 FR 51718, Aug. 31, 2006; 72 FR 20223, Apr. 24, 2007; 72 FR 62532, Nov. 5, 2007; 74 FR 2357, Jan. 15, 2009; 75 FR 14340, Mar. 25, 2010]

SUPPLEMENT NOS. 3–4 TO PART 742 [RESERVED]

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.)

[75 FR 36497, June 25, 2010]

SUPPLEMENT NO. 6 TO PART 742—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 describes 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