(C) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied. Contract sanctity date for reexports by non-U.S. persons: March 21, 2003.

(D) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: March 21, 2003.

(40) *''Software'' described in ECCN 2D983 specially designed or modified for the ''development'', ''production'' or ''use'' of explosives detection equipment.*

(i) [Reserved]

(ii) *Syria.* Applications for all end-users in Syria of these items will generally be denied. Contract sanctity date: March 21, 2003.

(iii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied. Contract sanctity date for reexports by non-U.S. persons: March 21, 2003.

(iv) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: March 21, 2003.

(41) *''Technology'' described in ECCN 2E983 specially designed or modified for the ''development'', ''production'' or ''use'' of explosives detection equipment.*

(i) [Reserved]

(ii) *Syria.* Applications for all end-users in Syria of these items will generally be denied. Contract sanctity date: March 21, 2003.

(iii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied. Contract sanctity date for reexports by non-U.S. persons: March 21, 2003.

(iv) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: March 21, 2003.

(42) *Production technology controlled under ECCN 1C355 on the CCL— .*

(i) [Reserved]

(ii) *Syria.* Applications for military end-users or for military end-uses in Syria of these items will generally be denied. Applications for non-military end-users or for non-military end-uses in Syria will be considered on a case-by-case basis.

(iii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied.

(iv) *North Korea.* Applications for military end-users or for military end-uses in North Korea of these items will generally be denied. Applications for non-military end-users or for non-military end-uses will be considered on a case-by-case basis.

(43) *Commercial Charges and devices controlled under ECCN 1C992 on the CCL.*

(i) [Reserved]

(ii) *Syria.* Applications for all end-users in Syria of these items will generally be denied.

(iii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied.

(iv) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied.

(44) *Ammonium nitrate, including certain fertilizers containing ammonium nitrate, under ECCN 1C997 on the CCL*

(i) [Reserved]

(ii) *Syria.* Applications for all end-users in Syria of these items will generally be denied. Contract sanctity date: June 15, 2001.

(iii) *Sudan.* Applications for all end-users in Sudan of these items will generally be denied.

(iv) *North Korea.* Applications for all end-users in North Korea of these items will generally be denied. Contract sanctity date: June 15, 2001.

(45) *Specific processing equipment, materials and software controlled under ECCNs 0A999, 0B999, 0D999, 1A999, 1C999, 1D999, 2A999, 2B999, 3A999, and 6A999 on the CCL.*

(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]

[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]

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

SUPPLEMENT NO. 5 TO PART 742—CHECKLIST ON ENCRYPTION AND OTHER ''INFORMATION SECURITY'' FUNCTIONS

1. Does your product perform ''cryptography'', or otherwise contain any parts or components that are capable of performing any of the following ''information security'' functions?

(Mark with an ''X'' all that apply)

a. ____ encryption
b. ____ decryption only (no encryption)
c. ____ key management/public key infrastructure (PKI)
d. ____ authentication (*e.g.*, password protection, digital signatures)
e. ____ copy protection
f. ____ anti-virus protection
g. ____ other (please explain) :_____
h. ____ NONE/NOT APPLICABLE

2. For items with encryption, decryption and/or key management functions (1.a, 1.b, 1.c above):

a. What symmetric algorithms and key lengths (*e.g.*, 56-bit DES, 112/168-bit Triple-DES, 128/256-bit AES/Rijndael) are implemented or supported?

b. What asymmetric algorithms and key lengths (*e.g.*, 512-bit RSA/Diffie-Hellman, 1024/2048-bit RSA/Diffie-Hellman) are implemented or supported?

c. What encryption protocols (*e.g.*, SSL, SSH, IPSEC or PKCS standards) are implemented or supported?

d. What type of data is encrypted?

3. For products that contain an ''encryption component'', can this encryption component be easily used by another product, or accessed by the end-user for cryptographic use?

[68 FR 35785, June 17, 2003, as amended at 73 FR 68325, Nov. 18, 2008]

SUPPLEMENT NO. 6 TO PART 742—GUIDELINES FOR SUBMITTING REVIEW REQUESTS FOR ENCRYPTION ITEMS

Review requests for encryption items must include all of the documentation described in this supplement and be submitted to BIS in accordance with §§748.1 and 748.3 of the EAR. To ensure that your review request is properly routed, insert the phrase ''Mass market encryption'', ''License Exception ENC'' or ''Other Encryption'' (whichever is applicable) in Block 9 (Special Purpose) of the application form and place an ''X'' in the box marked ''Classification Request'' in Block 5 (Type of Application)—Block 5 does not provide a separate item to check for the submission of encryption review requests. Failure to properly complete these items may delay consideration of your review request.

In addition, you must send a copy of your review request and all support documents to: Attn: ENC Encryption Request Coordinator, 9800 Savage Road, Suite 6940, Fort Meade, MD 20755–6000.

If you intend to rely on the 30 day registration provisions of the regulations, express mail certification of these documents is needed.

(a) For all review requests of encryption items, you must provide brochures or other documentation or specifications related to the technology, commodity or software, relevant product descriptions, architecture specifications, and as necessary for the technical review, source code. In addition, you must provide the following information in a cover letter accompanying your review request:

(1) State the name(s) of each product being submitted for review and provide a brief non-technical description of the type of product (*e.g.*, routers, disk drives, cell phones, chips, etc.) being submitted.

(2) Indicate whether there have been any prior reviews of the product(s), if such reviews 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, Application Control Number (ACN), 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, internal data, etc.).

(4) For mass market review requests, 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) State that a duplicate copy has been sent to the ENC Encryption Request Coordinator;

(c) For review requests for a 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, ECCN, 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