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

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) License Exception ENC 'Restricted' commodities and software described by the criteria in §740.17(b)(2) require licenses to certain ''government end-users.'' Describe whether the product(s) meet 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). If the §740.17(b)(2) parameters are not applicable to the commodity or software, clearly explain why (*e.g.*, by providing specific data evaluated against the §740.17(b)(2) thresholds.)

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

(d) For review 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.

(e) For review requests for ''encryption source code'' provide the following information:

(1) If applicable, reference the executable (object code) product that was previously reviewed;

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

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

(f) For step-by-step instructions and guidance on submitting review requests for encryption items, visit our webpage at *www.bis.doc.gov/Encryption* and click on the navigation button labeled ''Guidance''.

[67 FR 38868, June 6, 2002, as amended at 69 FR 71363, Dec. 9, 2004; 70 FR 22249, Apr. 29, 2005; 73 FR 49329, Aug. 21, 2008; 73 FR 57508, Oct. 3, 2008; 74 FR 52884, Oct. 15, 2009]

SUPPLEMENT NO. 7 TO PART 742—DESCRIPTION OF MAJOR WEAPONS SYSTEMS

(1) Battle Tanks: Tracked or wheeled self-propelled armored fighting vehicles with high cross-country mobility and a high-level of self protection, weighing at least 16.5 metric tons unladen weight, with a high muzzle velocity direct fire main gun of at least 75 millimeters caliber.

(2) Armored Combat Vehicles: Tracked, semi-tracked, or wheeled self-propelled vehicles, with armored protection and cross-country capability, either designed and equipped to transport a squad of four or more infantrymen, or armed with an integral or organic weapon of a least 12.5 millimeters caliber or a missile launcher.

(3) Large-Caliber Artillery Systems: Guns, howitzers, artillery pieces combining the characteristics of a gun or a howitzer, mortars or multiple-launch rocket systems, capable of engaging surface targets by delivering primarily indirect fire, with a caliber of 75 millimeters and above.

(4) Combat Aircraft: Fixed-wing or variable-geometry wing aircraft designed, equipped, or modified to engage targets by employing guided missiles, unguided rockets, bombs, guns, cannons, or other weapons of destruction, including versions of these aircraft which perform specialized electronic warfare, suppression of air defense or reconnaissance missions. The term ''combat aircraft'' does not include primary trainer aircraft, unless designed, equipped, or modified as described above.

(5) Attack Helicopters: Rotary-wing aircraft designed, equipped or modified to engage targets by employing guided or unguided anti-armor, air-to-surface, air-to-subsurface, or air-to-air weapons and equipped with an integrated fire control and aiming system for these weapons, including versions of these aircraft that perform specialized reconnaissance or electronic warfare missions.

(6) Warships: Vessels or submarines armed and equipped for military use with a standard displacement of 750 metric tons or above, and those with a standard displacement of less than 750 metric tons that are equipped for launching missiles with a range of at least 25 kilometers or torpedoes with a similar range.

(7) Missiles and Missile Launchers:

(a) Guided or unguided rockets, or ballistic, or cruise missiles capable of delivering