GUIDELINES FOR SUBMITTING REVIEW REQUESTS FOR ENCRYPTION ITEMS

Review requests for encryption items must be submitted on Form BIS-748P (Multipurpose Application), or its electronic equivalent, and supported by the documentation described in this Supplement, in accordance with the procedures described in §748.3 of the EAR. To ensure that your review request is properly routed, insert the phrase "Mass market encryption" or "License Exception ENC" (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. BIS recommends that review requests be delivered via courier service to: Bureau of Industry and Security, U.S. Department of Commerce, 14th Street and Pennsylvania Ave., N.W., Room 2705, Washington, D.C. 20230. For electronic submissions via SNAP, you may fax a copy of the support documents to BIS at (202) 219-9179 or -9182 or you may deliver the documents via courier service to: Bureau of Industry and Security, Information Technology Controls Division, Room 2625, 14th Street and Pennsylvania Ave., N.W., Washington, D.C. 20230. 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 6131, Fort Meade, MD 20755-6000. 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. You must also indicate whether there have been any prior reviews of the product, if such reviews are applicable to the current submission. In addition, you must provide the following information in a cover letter accompanying your review request:

(a) State the name of the encryption item being submitted for review.

(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. 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 the communication protocols (e.g., X.25, Telnet or TCP) and encryption protocols (e.g., SSL, IPSEC or PKCS standards) that are supported.

(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 whether the cryptographic routines are statically or dynamically linked, and the routines (if any) that are provided by third-party modules or libraries. Identify the third-party manufacturers of the modules or toolkits.

(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) For products that qualify as "retail", explain how the product meets the listed criteria in §740.17(b)(3) of the EAR.

(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 regarding components, 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 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.gov/Encryption and click on the navigation button labeled "Guidance".