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

a warhead or weapon of destruction to a range of at least 25 kilometers, and those items that are designed or modified specifically for launching such missiles or rockets, if not covered by systems identified in paragraphs (1) through (6) of this Supplement. For purposes of this rule, systems in this paragraph include remotely piloted vehicles with the characteristics for missiles as defined in this paragraph but do not include ground-to-air missiles;

(b) Man-Portable Air-Defense Systems (MANPADS); or

(c) Unmanned Aerial Vehicles (UAVs) of any type, including sensors for guidance and control of these systems, except model airplanes.

(8) Offensive Space Weapons: Systems or capabilities that can deny freedom of action in space for the United States and its allies or hinder the United States and its allies from denying an adversary the ability to take action in space. This includes systems such as anti-satellite missiles, or other systems designed to defeat or destroy assets in space.

(9) Command, Control, Communications, Computer, Intelligence, Surveillance, and Reconnaissance (C4ISR): Systems that support military commanders in the exercise of authority and direction over assigned forces across the range of military operations; collect, process, integrate, analyze, evaluate, or interpret information concerning foreign countries or areas; systematically observe aerospace, surface or subsurface areas, places, persons, or things by visual, aural, electronic, photographic, or other means; and obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy, or secure data concerning the meteorological, hydrographic, or geographic characteristics of a particular area, including Undersea communications. Also includes sensor technologies.

(10) Precision Guided Munitions (PGMs), including ''smart bombs'': Weapons used in precision bombing missions such as specially designed weapons, or bombs fitted with kits to allow them to be guided to their target.

(11) Night vision equipment: Any electro-optical device that is used to detect visible and infrared energy and to provide an image. This includes night vision goggles, forward-looking infrared systems, thermal sights, and low-light level systems that are night vision devices, as well as infrared focal plane array detectors and cameras specifically designed, developed, modified, or configured for military use; image intensification and other night sighting equipment or systems specifically designed, modified or configured for military use; second generation and above military image intensification tubes specifically designed, developed, modified, or configured for military use, and infrared, visible and ultraviolet devices specifically designed, developed, modified, or configured for military application.

[72 FR 33656, June 19, 2007, as amended at 73 FR 58037, Oct. 6, 2008]

PART 743—SPECIAL REPORTING

Sec.

AUTHORITY: 50 U.S.C. app. 2401 *et seq.*; 50 U.S.C. 1701 *et seq.*; E.O. 13222, 66 FR 44025, 3 CFR, 2001 Comp., p. 783; Notice of August 13, 2009, 74 FR 41325 (August 14, 2009).

SOURCE: 63 FR 2458, Jan. 15, 1998, unless otherwise noted.

§ 743.1 Wassenaar Arrangement.

(a) *Scope.* This section outlines special reporting requirements for exports of certain commodities, software and technology controlled under the Wassenaar Arrangement. Such reports must be submitted to BIS semiannually in accordance with the provisions of paragraph (f) of this section, and records of all exports subject to the reporting requirements of this section must be kept in accordance with part 762 of the EAR. This section does not require reports for reexports.

NOTE TO PARAGRAPH (a) OF THIS SECTION: For purposes of part 743, the term ''you'' has the same meaning as the term ''exporter'', as defined in part 772 of the EAR.

(b) *Requirements.* You must submit two (2) copies of each report required under the provisions of this section and maintain accurate supporting records (see §762.2(b) of the EAR) for all exports of items specified in paragraph (c) of this section for the following:

(1) Exports authorized under License Exceptions GBS, CIV, TSR, LVS, APP, and the cooperating government portions (§§740.11(b)(2)(iii) and 740.11(b)(2)(iv) of the EAR) of GOV (see part 740 of the EAR). Note that exports of technology and source code under License Exception TSR to foreign nationals located in the U.S. should not be reported; and