(4) Identify the encryption component and include the name of the manufacturer, component model number or other identifier.

(d) For classification requests for ''encryption source code'' provide the following information:

(1) If applicable, reference the executable (object code) product that was previously classified by BIS or included in an encryption registration to BIS;

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

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

[75 FR 36497, June 25, 2010]

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]

SUPPLEMENT NO. 8 TO PART 742—SELF-CLASSIFICATION REPORT FOR ENCRYPTION ITEMS

This supplement provides certain instructions and requirements for self-classification reporting to BIS and the ENC Encryption Request Coordinator (Ft. Meade, MD) of encryption commodities, software and components exported or reexported pursuant to encryption registration under License Exception ENC (§740.17(b)(1) only) or ''mass market'' (§742.15(b)(1) only) provisions of the EAR. See §742.15(c) of the EAR for additional instructions and requirements pertaining to this supplement, including when to report and how to report.

(a) *Information to report.* The following information is required in the file format as described in paragraph (b) of this supplement, for each encryption item subject to the requirements of this supplement and §§740.17(b)(1) and 742.15(b)(1) of the EAR:

(1) Name of product (50 characters or less).

(2) Model/series/part number (50 characters or less.) If necessary, enter 'NONE' or 'N/A'.

(3) Primary manufacturer (50 characters or less). Enter 'SELF' if you are the primary manufacturer of the item. If there are multiple manufacturers for the item but none is clearly primary, either enter the name of one of the manufacturers or else enter 'MULTIPLE'. If necessary, enter 'NONE' or 'N/A'.

(4) Export Control Classification Number (ECCN), selected from *one* of the following:

(i) 5A002
(ii) 5B002
(iii) 5D002
(iv) 5A992
(v) 5D992

(5) Encryption authorization type identifier, selected from *one* of the following, which denote eligibility under License Exception ENC (§740.17(b)(1), only) or as 'mass market' (§742.15(b)(1), only):

(i) ENC
(ii) MMKT

(6) Item type descriptor, selected from *one* of the following:

(i) Access point
(ii) Cellular
(iii) Computer
(iv) Computer forensics
(v) Cryptographic accelerator
(vi) Data backup and recovery
(vii) Database
(viii) Disk/drive encryption
(ix) Distributed computing
(x) E-mail communications
(xi) Fax communications
(xii) File encryption
(xiii) Firewall
(xiv) Gateway
(xv) Intrusion detection
(xvi) Key exchange
(xvii) Key management
(xviii) Key storage
(xix) Link encryption
(xx) Local area networking (LAN)
(xxi) Metropolitan area networking (MAN)
(xxii) Modem
(xxiii) Network convergence or infrastructure n.e.s.
(xxiv) Network forensics
(xxv) Network intelligence
(xxvi) Network or systems management (OAM/OAM&P)
(xxvii) Network security monitoring
(xxviii) Network vulnerability and penetration testing
(xxix) Operating system
(xxx) Optical networking
(xxxi) Radio communications
(xxxii) Router
(xxxiii) Satellite communications
(xxxiv) Short-range wireless n.e.s.
(xxxv) Storage area networking (SAN)
(xxxvi) 3G/4G/LTE/WiMAX
(xxxvii) Trusted computing
(xxxviii) Videoconferencing
(xxxix) Virtual private networking (VPN)
(xl) Voice communications n.e.s.
(xli) Voice over Internet protocol (VoIP)
(xlii) Wide area networking (WAN)
(xliii) Wireless local area networking (WLAN)
(xliv) Wireless personal area networking (WPAN)
(xlv) Commodities n.e.s.
(xlvi) Components n.e.s.
(xlvii) Software n.e.s.
(xlviii) Test equipment n.e.s.
(xlix) OTHER

(b) *File format requirements.* (1) The information described in paragraph (a) of this supplement must be provided in tabular or spreadsheet form, as an electronic file in comma separated values format (.csv), only. No file formats other than .csv will be accepted, as your encryption self-classification report must be directly convertible to tabular or spreadsheet format, where each row (and all entries within a row) properly correspond to the appropriate encryption item.