SHEPPARD MULLIN
SHEPPARD MULLIN RICHTER & HAMPTON LLP
Government Contracts Law BLOG
For the latest updates on laws affecting government contracts

Government Contracts Blog

Posted at 11:26 AM on March 12, 2010 by Sheppard Mullin

Stay Tuned for Implementation of Ancillary Cryptography Changes Adopted by December 2009 Wassenaar Plenary Session

At their December 2009 Plenary Session, the member countries of the Wassenaar Arrangement on dual-use export controls adopted a new Note 4 to Category 5 - Part 2 of the Dual-Use List covering information security and encryption.

The new note provides that Category 5–Part 2 does not apply to items incorporating or using "cryptography" if:

a. The primary function or set of functions is not any of the following:

1. "Information security";

2. A computer, including operating systems, parts and components therefor;

3. Sending, receiving or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management); or

4. Networking (includes operation, administration, management and provisioning);

b. The cryptographic functionality is limited to supporting their primary function or set of functions; and

c. When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority in the exporter's country in order to ascertain compliance with conditions described in paragraphs a. and b. above.

This change will soon be implemented in the United States, and it represents an interesting variation on the "ancillary cryptography" exception published by the Commerce Department's Bureau of Security in October 2008. See Encryption Simplification, 73 Fed. Reg. 57,495 et seq. (Oct. 3, 2008). That action eliminated the requirement of a review request filing and twice-a-year reporting under the ENC license exception, 15 C.F.R. sec. 740.17 (2009), but retained the 5D002 classification for items with ancillary cryptography.

The 2008 U.S. action introduced the following definition of ancillary cryptography which included a Nota Bene with a laundry list of examples to illustrate products that qualify for self-classification as ancillary:

> ***Ancillary Cryptography.*** The incorporation or application of ‘‘cryptography’’ by items that are not primarily useful for computing (including the operation of ‘‘digital computers’’), communications, networking (includes operation, administration, management and provisioning) or ‘‘information security’’. **N.B.** Commodities and software that perform ‘‘ancillary cryptography’’ (e.g., are specially designed and limited to: piracy and theft prevention for software, music, etc.; games and gaming; household utilities and appliances; printing, reproduction, imaging and video recording or playback (but not videoconferencing); business process modeling and automation (e.g., supply chain management, inventory, scheduling and delivery); industrial, manufacturing or mechanical systems (including robotics, other factory or heavy equipment, facilities systems controllers including fire alarms and HVAC); automotive, aviation and other transportation systems). Commodities and software included in this description are not limited to wireless communication and are not limited by range or key length.

Note 4 as adopted by the Wassenaar Plenary carries forward the U.S. definition of products with "ancillary cryptography" as those whose primary purpose is not information security, computing, communications or networking, but it goes further by removing them entirely from Category 5 – Part 2. In this respect, they become like "[c]ommodities and software specially designed for medical end-use," which are excluded from Category 5 – Part 2 by current Note 1. See 15 C.F.R. pt. 774, supp. 1 at page 754 (2009).

Unlike the U.S. rule from 2008, however, the Wassenaar Note 4 omits the list of examples in the Nota Bene published by the Commerce Department in October 2008. It is not clear at this time whether some Wassenaar members will implement Note 4 in a manner that differs from these examples previously published in the United States.

What is clear is that a new regulation can be expected this year to implement this change in the United States. Commerce officials foreshadowed this in public statements at their Update 2009 Conference Encryption Workshop on October 2, 2009. See here, at page 29 ("As you probably know, the Wassenaar meets in plenary in December, and we anticipate that the note four will be implemented and published soon after the December plenary in the Wassenaar lists, and we thought it was an important enough development to mention it here today").

The 2008 Wassenaar Plenary changes were not published in the Federal Register until December 2009, 74 Fed. Reg. 65,999 et seq. (Dec. 11, 2009), so the publication of Note 4 may not occur very soon, but when it does exporters will be spared the task of remembering that their decontrolled items containing encryption for ancillary purposes remain classified as 002 and require reliance on the ENC license exception. An interesting further consequence of the change will be that many items with ancillary cryptography will end up becoming EAR99. This will have an impact on some reexport scenarios.

One must wonder about the logic of excluding ancillary cryptography in this manner while items with encryption limited to password protection and user authentication remain in 992. Heretofore, exporters have done well to consider first whether an encryption function is limited to password protection or user authentication. Under Note 4, they will want to retool their decision trees to start with the ancillary exception since it will take items outside of Category 5, Part 2 altogether.

Authored by:

Curtis Dombek
(213) 617-5595
cdombek@sheppardmullin.com