# Export Update

A Newsletter for Clients of Sharretts, Paley, Carter & Blauvelt, P.C. July 1, 2010

## *New BIS Interim Final Rule Makes Changes to Encryption Controls*

The Department of Commerce, Bureau of Industry and Security ("BIS") issued an interim final rule, effective June 25 modifying the requirements of the export license applicable to encryption commodities, software, and related technology, exception "ENC".

The new rule is one of the first steps in President Obama's plan to reform U.S. export controls and enhance national security.

The following are among the changes promulgated by the new rule:

**Immediate Export Authorization for Certain Products**

The new rule eliminates the requirement to wait 30 days for a technical review before exporting certain encryption products of lesser national security concern and mass market encryption products. Instead, such items may be immediately authorized for export and reexport after electronic submission of a company's encryption registration to BIS. Companies utilizing this type of authorization will be required to file an annual self-classification report, detailing software and commodities exported under exception ENC.

Covered products include those classified in new Export Control Classification Numbers ("ECCNs") 5A002.1.1, .a.2, .a.5, .a.6, or .a.9, or ECCN 5B002, and certain equivalent or related software classified under ECCN 5D002. Covered "mass market" products are those that meet all of the following requirements:

1) Generally available to the public by being sold, without restriction, from stock at retail selling points by means of any of the following:
    a. Over-the-counter transactions;
    b. Mail order transactions;
    c. Electronic transactions; or

SHARRETTS, PALEY, CARTER & BLAUVELT, P.C.

75 Broad Street
New York, New York 10004
Phone: 212-425-0055
Fax: 212-425-1797
212-742-2180

www.spcblaw.com
*Email:* customs@sharretts-paley.com

1660 L Street, N.W.
Washington, D.C. 20036
Phone: 202-223-4433
Fax: 202-659-3904

   d. Telephone call transactions;
2) The cryptographic functionality cannot be easily changed by the user;
3) Designed for installation by the user without further substantial support by the supplier; and
4) When necessary, details of the items are accessible and will be provided, upon request, to the appropriate authority.

**Elimination of Redundant Encryption Classification Request Requirements**

The rule eliminates the requirement to file separate encryption classification requests with both BIS and the ENC Encryption Request Coordinator in Fort Meade, Maryland. Classification requests filed with BIS via the Simplified Network Application Processing system, ("SNAP-R") will automatically be forwarded to the ENC Encryption Request Coordinator. All reports (such as the semi-annual sales report and the annual self-classification report) must continue to be submitted to both BIS and the ENC Encryption Request Coordinator.

**New ENC Eligibility for Most Encryption Technology to Non-Government-End-Users**

Encryption technology classified under ECCN 5E002 that is not technology for "cryptanalytic items," "non-standard cryptography," or "open cryptographic interfaces" may now be exported and reexported under exception ENC to any non-government end user located in a country not listed in Country Groups D:1 or E:1.

"Cryptanalytic items" is defined as "systems, equipment, applications, specific electronic assemblies, modules and integrated circuits designed or modified to perform cryptanalytic functions, software having the characteristics of cryptanalytic hardware or performing cryptanalytic functions, or technology for the development, production or use of cryptanalytic commodities or software."

"Non-standard cryptography" is defined as "any implementation of cryptography involving the incorporation or use of proprietary or unpublished cryptographic functionality, including encryption algorithms or protocols that have not been adopted or approved by a duly recognized international standards body (e.g., IEEE, IETF, ISO, ITU, ETSI, 3GPP, TIA, AND GSMA) and have not otherwise been published."

"Open cryptographic interfaces" is defined as "a mechanism which is designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces." Open cryptographic interfaces may not contain a fixed set of cryptographic algorithms, key lengths or key exchange management systems that cannot be changed. All general application programming interfaces (e.g., those that accept either a cryptographic or non-cryptographic interface but do not themselves maintain any cryptographic functionality) will not be considered 'open' cryptographic interfaces.

The destination countries still requiring licenses include Albania, Armenia, Azerbaijan, Belarus, Burma, Cambodia, China, Cuba, Georgia, Iraq, Iran, Kazakhstan, North Korea, Kyrgyzstan, Laos, Libya, Macau, Moldova, Mongolia, Russia, Sudan, Syria, Tajikistan, Turkmenistan, Ukraine, Uzbekistan, and Vietnam.

**Changes in ECCN 5A002 Relating to Smart Cards**

The new rule rewords portions of the note explaining ECCN 5A002. The portion of the note relating to personalized smart cards was removed and replaced with one stating that smart cards and smart card

readers/writers are controlled under 5A992 if the cryptographic capability is restricted in certain systems and they meet the following requirements:

1) The cryptographic capability is restricted for use in equipment or systems excluded from 5A002,
2) The devices have all of the following:
    a. Specifically designed and limited to allow protection of 'personal data' stored within;
    b. Has been, or can only be, personalized for public or commercial transactions or individual identification; and
    c. Where the cryptographic capability is not user-accessible.

**"Information Security" Items Excluded from Control**

A new note to Category 5, Part 2 of the Commerce Control List ("CCL") excludes items that incorporate or use cryptography from Category 5, Part 2 control if the item's primary function or set of functions is not "information security," computing, communications, storing information, or networking, and if the cryptographic function in the item only serves to support such functions. As a result, items supporting entertainment, mass commercial broadcasts, digital rights management, medical records management, and others are now excluded from Category 5, Part 2 control. Specific examples of such items include piracy prevention for software or music, games, video and image recording or playback devices, business process management tools, manufacturing or mechanical systems, transportation systems, HDMI and component video interfaces, medical office applications, academic instruction tools and software, applied geosciences equipment, scientific simulation devices, computer aided design software, and household appliances. Such items should now be evaluated under other categories of the CCL to determine if other controls apply. If the item is not controlled under another category of the CCL, then it should be designated as EAR99.

Comments on the new rule are due to BIS by August 24, 2010. Please contact Gail T. Cumins at 212-425-0055 or gcumins@spcblaw.com if you are interested in having us submit comments on your behalf.