COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Foreign Trade Controls

July 6, 2010

AMENDMENTS TO THE ENCRYPTION PROVISIONS OF THE EXPORT ADMINISTRATION REGULATIONS TRANSFORM THE EXISTING PRODUCT-BY-PRODUCT "REVIEW-AND-WAIT" PROCEDURES TO A STREAMLINED "REGISTRATION-AND-ANNUAL-REPORT" PROCESS

THE AMENDMENTS IMPLEMENT AN EXPORT REFORM INITIATIVE ANNOUNCED IN MARCH

On Friday, June 25, the Department of Commerce, Bureau of Industry and Security (BIS) issued interim final regulations amending the encryption provisions of the Export Administration Regulations (EAR). Although BIS is accepting public comments until August 24, the new amendments are effective immediately upon publication.

Products that use encryption to ensure security of information — including widely-used software such as web browsers, desktop applications, and operating systems, and hardware such as cell phones, internet routers, and networking equipment — have long been singled out for special treatment under the EAR, with more stringent and more cumbersome procedures for classification to qualify for export or reexport. The amended regulations are designed to streamline EAR procedures for most mass market encryption products and other less sensitive encryption items. In addition, the new rules decontrol items that perform only "ancillary cryptography."

President Obama previewed these encryption amendments in a March 2010 speech outlining his National Export Initiative, which is designed to support the Administration's goal of doubling exports over the next five years. According to the Administration, the revisions will streamline export requirements for roughly 2,800 mass-market encryption products including many laptops, software applications, disk drives, mobile phones, local area network (LAN) products, and small routers, and will decrease the burden on both exporters and BIS by eliminating approximately 70 percent of required encryption technical reviews and up to 85 percent of semi-annual reporting that is now required.

Review Requirements Prior to These Amendments

Previously, before an item with encryption could be exported to any destination other than Canada, the EAR required the manufacturer, developer, or other exporter to submit technical information about the product to BIS and to the ENC Encryption Request Coordinator at the National Security Agency (NSA) for a one-time, 30-day technical review and classification to determine its Export Control Classification Number (ECCN) on the EAR's Commerce Control List and its eligibility for export. Based on that review, the product could become qualified for export to all destinations other than terrorist-supporting countries under one of three paths, depending on the nature of the product and the ECCN:

1. Mass market encryption items became eligible for export "no license required" (NLR) after review. "Mass market" encryption products are those sold in large quantities and generally available to the public through common retail methods.
2. Other encryption items that do not qualify as mass market but are still considered non-sensitive based on performance characteristics became eligible for export pursuant to License Exception ENC to both government and non-government end-users. These are generally referred to as "ENC Unrestricted" products.
3. Sensitive encryption items that exceed certain functional or performance criteria became eligible for License Exception ENC export to non-government end-users in all but terrorist-supporting countries, but required specific licensing for export to government end-users in many countries. These are generally referred to as "ENC Restricted" products.

Under the prior procedures, each product (both hardware and software) had to be separately submitted for this technical review to qualify for export as outlined above. Absent changes to the encryption features, only one review was required for each product, however, so that a developer's customers could export the product after the developer submitted the product for the one-time technical review and classification. In addition, exporters were required to file semi-annual reports with details concerning many of the exports made under License Exception ENC (with some exceptions). This semi-annual reporting requirement did not apply to NLR (mass markets) exports, however.

Streamlined Review and Reporting Requirements

The new rule replaces this product-by-product review procedure with a one-time registration and annual reporting procedure for most mass market products and ENC Unrestricted products that use standard encryption algorithms and protocols. By contrast, sensitive ENC Restricted encryption products, and even some less sensitive encryption components or items with proprietary and/or non-standard encryption, do not qualify for this streamlined process, and will still require prior classification review before qualifying for export, as discussed in the final section below.

The new streamlined process provides immediate authorization to export and reexport encryption products after an exporter/manufacturer has electronically submitted an encryption registration to BIS. The registration form must identify the company/registrant, the general categories or "families" of encryption products it makes or exports, and whether those products use proprietary, unpublished or other "non-standard" encryption. Notably, however, in contrast to the previous review procedures, the registration need not identify specific products or describe specific encryption algorithms or protocols used. BIS will then issue the exporter/manufacturer an "encryption registration number" (ERN) that immediately authorizes export and reexport, by anyone, of that company's qualifying mass market encryption products (as NLR exports) and ENC Unrestricted encryption products (under License Exception ENC) to destinations other than terrorist-supporting countries (but excluding exports or reexports to prohibited end-users or end-uses). In other words, once a manufacturer or producer of an encryption item has registered and received its ERN, the registered company's customers or other third parties may export or reexport in reliance on the ERN and classification information provided by the registered company, and will not be required to register separately with BIS.

An exporter who takes advantage of this authority must, however, submit an annual self-classification report identifying, describing and classifying (by ECCN) each of the encryption commodities and software that it has exported in the prior year. The report is due no later than February 1 for the past calendar year. This annual report replaces (for these exports) the previous

requirement to file semi-annual post-export reports with details concerning sales, quantities, and distribution.

Decontrol of "Ancillary Cryptography" Items

The previous rules already exempted from the prior classification review requirements those items that incorporate or employ only "ancillary cryptography" — i.e., products that are not primarily useful for general computing, communications, networking or information security. Implementing a December 2009 agreement among Wassenaar Arrangement member countries, the revised rule now completely decontrols such "ancillary cryptography" items, removing them from the scope of encryption ECCNs. A new note to Category 5, Part 2 ("Information Security") of the Commerce Control List now excludes products where (a) the encryption functionality is limited to supporting the product's primary function; and (b) the primary function or set of functions is not one of the following: Information security; a computer (including operating systems, parts and components); networking; or sending, receiving, or storing information (except in support of entertainment, mass commercial broadcasts, digital rights management or medical records management).

Examples of items that are no longer subject to the encryption ECCNs in Category 5, Part 2, include piracy and theft prevention for software or music; games and gaming; household appliances; robotics; imaging and video recording or playback; industrial, manufacturing or mechanical systems; inventory management software; and LCD TV, Blu-ray/DVD, and video on demand (VoD). Exporters and producers may now self-classify these items (and others excluded by the note above) under another, non-encryption ECCN or as EAR99. As a result of the decontrol of these items, the revision removes all references to the term "ancillary cryptography" from the EAR.

Encryption Items and Technology Still Subject to Classification Review Prior to Export

As noted, all ENC Restricted items continue to be subject to the 30-day classification review requirements to qualify for License Exception ENC, and exporters of such products must still comply with requirements for semi-annual reporting concerning exports of such items. ENC Restricted items include some network infrastructure items — such as routers and 3G wireless base stations — that exceed certain technical performance parameters.

In addition, certain mass market and ENC Unrestricted items do not qualify for the streamlined ERN process described above, and remain subject to the 30-day classification review requirements to qualify for export and the semi-annual reporting requirements. These are (1) "encryption components," (2) items that provide or perform "non-standard cryptography," (3) forensics tools, and (4) cryptographic enabling items.

1. "Encryption components" include chips, chipsets, electronic assemblies and field programmable logic devices; and cryptographic modules, libraries, development kits and toolkits.
2. "Non-standard cryptography" means proprietary or unpublished cryptographic algorithms or protocols, including cryptography that has not been adopted or approved by duly recognized international standards bodies and has not otherwise been published.
3. Forensics tools include those providing or performing vulnerability analysis, network forensics or computer forensics.
4. Cryptographic enabling items means commodities and software that activate or enable encryption functionality in other products which would otherwise remain disabled.

The EAR revision also continues to require a 30-day technical review for export and reexport of many types of encryption technology necessary for the development and use of encryption products. The

scope of License Exception ENC for such exports has been expanded in one respect but apparently made more restrictive in another respect. Under previous regulations, encryption technology could be exported immediately upon submission of a technical review request, but only to the 35 countries named in Supplement 3 to EAR Part 742. The revised rule makes most encryption technology (except "non-standard cryptographic," "cryptanalytic" and "open cryptographic interface" technology) eligible for ENC export to more countries (all except Group E:1 terrorist-supporting countries and countries of national security concern designated in Group D:1), but apparently now only after a 30-day waiting period rather than immediately upon submission of the classification review request.

The revised rule does eliminate the requirement for separate hard-copy submission of encryption classification requests to the Encryption Request Coordinator at NSA. BIS will instead electronically forward encryption classification requests to the Encryption Request Coordinator.

As noted, the new rules take effect immediately, but BIS is nonetheless seeking public comments, which must be received by August 24, 2010.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our foreign trade controls practice group:

Peter Flanagan	202.662.5163	pflanagan@cov.com
David Addis	202.662.5182	daddis@cov.com
Corinne Goldstein	202.662.5534	cgoldstein@cov.com
Kimberly Strosnider	202.662.5816	kstrosnider@cov.com
Christine Minarich	202.662.5106	cminarch@cov.com