Guest View

BY GRAYSON YEARGIN

Grayson Yeargin, a partner in the Washington office of law firm Jones Day, was assisted by associate Chase Kaniecki.

Encryption export controls explained

As global trading explodes, U.S. software companies are expanding their sales and product development internationally. Whether it's a small company beginning to sell internationally or a sophisticated company looking to outsource product development, one issue often overlooked or misunderstood is how encryption functionally can impact, and in some cases restrict, international activities.

Export issues can arise when selling to customers outside the United States, or when customers request information relating to the export control status of products. They can also appear during due diligence when a software company is the target of an acquisition. We routinely hear misconceptions about U.S. encryption export controls, and here are six of those misconceptions:

1. "Our products do not contain or use encryption." Almost all software products contain encryption of some sort. Software may be controlled for encryption, even if the encryption is actually performed by the operating system, an external library, a third-party product, or a cryptographic processor. Further, if a product includes encryption functionality, even if that functionality is not used, the U.S. government evaluates the product based on the included encryption functionality. Such functionality may be there simply for copyright protection, in which case the product may not be subject to export controls. Encryption also may be present due to third-party licensing requirements, which could cause the product to be subject to export controls.

2. "The government doesn't care about this type of product." The government's interest isn't limited to the main purpose of the product; it also is interested in the product's components, libraries and capabilities. Commercial software is subject to export controls based on its classification under the Export Administration Regulations (EAR). To assess the applicable controls, one must determine the classification of the software's functional characteristics and its encryption functionality.

3. "I got this product from a major software developer, and they must have already done everything to make sure it's okay to export it." This misconception suffers from two flaws. First, it is important to confirm with a supplier whether the company has evaluated the export control status of its product and, if so, whether all regulatory requirements have been satisfied. Second, even if the U.S. government previously reviewed and classified an encryption software product, additional regulatory requirements may apply if the encryption functionality or other technical characteristics are altered when incorporated into another software product.

4. "We only utilize foreign-made encryption products." The U.S. export controls apply not only to U.S.-origin products, but also foreign-made products that come into the United States. Accordingly, if a U.S. software company procures a foreign-made encryption product, and incorporates it into its own product, it is possible that the final product would be subject to export controls.

5. "We registered with the U.S. government, so we're okay." Even companies that have classified their encryption products under the EAR can make mistakes in connection with exporting their products. For example, software companies often mistakenly believe that obtaining an encryption registration number allows them to export their products around the world without restriction. However, additional requirements, such as submitting classification requests prior to exporting, periodic reporting of exports, and restrictions on eligible customers also may apply to those products.

One issue often overlooked is how encryption can impact, and in some cases restrict, international acitivites.

6. "We classified our products a while ago, so we're good." This statement has two problems. First, software products regularly undergo updates. When updates alter encryption functionality, the export control status of the product should be re-evaluated. Second, in June 2010, the U.S. encryption export control regulations underwent a substantial overhaul. Software companies that evaluated the export control status of their products prior to June 2010 should consider re-evaluating those products under the amended regulations.

U.S. software companies engaging in international sales or development should evaluate the export control status of their products. This often requires reviewing the applicable regulations and determining whether the products are subject to export controls. Once that review is completed, a company must assess the nature and extent of any applicable requirements and ensure compliance with them. ▮

Read this story on sdtimes.com