On Second Thought
With Beth Peterson

Export warning to all startups

Many new startups are innovating products that include encryption — which is always subject to export controls. Because they aren't familiar with export regulations, companies inadvertently violate them when building new products; they don't know that all technology products require an export control classification number (ECCN) and possibly an export license. U.S. export regulations can apply domestically and follow U.S. origin goods as they ship around the world. We've found that many companies (not just startups) have little visibility into what export compliance means to their companies and what minimum level of compliance standards they must implement whether they export or not.

Encryption controls apply to hardware, software, and technology. Export controls govern the strategic distribution of goods to foreign nationals and countries for foreign policy and national security purposes.

So where do you start? The first question you should ask is whether your product contains encryption. This may sound simple, but you have to not only consider your item, but also any open source software and any third-party modules and libraries that might have been used. (We use an encryption questionnaire that is based on the government's questionnaire and we're happy to share ours with you. To give you a perspective on how complex encryption classification can be, our questionnaire can be up to 19 pages long depending on the product.)

You're probably hoping that your products still aren't subject to the encryption regulations. However, here's a non-inclusive list of examples of items and technology that are — products whose primary function is information security, computing, communications, storing information, or networking; software that contains SSL; printed circuit boards that contain a crypto-capable chip; a Chinese national developing software that contains symmetric encryption over 80-bits; Bluetooth headsets; foreign products developed with U.S.-origin encryption source code, components or toolkits; software containing source and/or object code; and LAN equipment being shipped to a foreign subsidiary.

If your product does contain encryption, here are some of the steps that you should follow:

1. Start with the U.S. Bureau of Industry and Security's website (**www.bis.doc.gov**) to get a broad understanding of encryption controls.

2. Familiarize yourself with the Export Administration Regulations (EAR), especially under Category 5, Part 2 — Information Security, Part 740.17 — License Exception ENC, and Part 742 — Control Policy — Commerce Control List-based controls.

3. Sign up for SNAP-R (Simplified Network Application Process — Redesign) for online encryption registration,

4. Obtain a Company Identification Number (CIN).

5. Obtain an Encryption Registration Number.

6. Determine the classification of your item and either:

a. Self-classify your product and report it (when allowed and required).

b. File a Commodity Classification Request (CCR) (when required).

c. Determine whether a license is required or if a license exception is available.

If your product requires a CCR or a license, you will need to apply for the CCR before you can export. Depending on the classification of your item, you may not be able to export or apply for a license until you received a CCR response. A CCR response from the Commerce Department can take up to 30 days or more. An export license application can take 20-40 days, or more, to receive an export license or denial. In addition to applying for and receiving export licenses, you may need to get end-user statements to support your license or license authorizations.

Once you have authorization to export your item (either via a license exception or an actual license) you will be subject to conditions to which you must adhere to be compliant. This could include reporting requirements, end-user visits, and/or other types of restrictions. You will also be required to put certain information on your export documentation and declarations and to recordkeeping requirements. You'll need to train your product management and engineering, logistics, order management and customer service teams on your encryption policy and procedures. And you'll have to repeat the whole process if you upgrade or develop new products. A written manual is best on top of regular employee training.

So far, we've just considered tangible products. In the case of technology, there's a rule regarding "deemed exports," which is providing foreign nationals controlled technology while they are here in the United States. The foreign national may require an export license to use or view the technology because he or she will at some point return home overseas and therefore "export" the technology with them. Whether an individual needs a license depends on his or her nationality and the type of technology. It behooves any company, even if they do not export physical product to at least classify their technologies, including software available for download (whether for sale or at no charge), to appropriately handle these types of legal liabilities.

As you can see, export compliance is involved in more than just shipping products internationally. Even domestic activities must adhere to U.S. export regulations. Export compliance must be an integral part of not only daily operations but also business development and strategy. Companies who ignore export compliance will most likely end up with penalties, fines, bad press or — even worse — the inability to export. Ensure your company avoids these risks by establishing an export compliance program. And remember, for any program to be successful, the message and commitment must come from the top.

Peterson is president of BPE Global, a global trade consulting and training firm. She can be reached by email at beth@bpeglobal.com.