License exception ‘ENC’ reporting requirements

As we’ve discussed here previously, recordkeeping is often overlooked in the midst of the operational chaos that dominates most of our day-to-day lives despite its importance when conducting audits. And the first step to tackling recordkeeping is understanding what regulatory agency requirements apply to your company.

Another area that could potentially be going unnoticed in your trade compliance department is that of encryption reporting.

As with recordkeeping, encryption reporting requires you to know what U.S. regulatory agencies’ reporting rules are applicable to your organization, such as those of the Bureau of Industry and Security and the National Security Agency.

Although the American Shipper readership is comprised of shippers, carriers and various third parties involved in international transportation, I would imagine most of you reading this have never submitted a semi-annual encryption report, nor an annual self-classification report. Even so, we can be fairly certain someone within your company has exported an encryption item during 2016.

The subject of encryption reporting is fresh in my mind, as the first deadline of 2017 was Feb. 1 and for those of us in trade compliance consulting, January is a bit like tax season is for accountants. Whether or not your company has a trade compliance function, or someone in shipping/logistics who does your export classifications, licensing, electronic export information (EEI) filings etc., management must be aware that encryption reporting is required for certain encryption exports.

You may not design or sell encryption items, but most companies in the U.S. today ship encryption items cross-border to support global operations. Items like software (including downloads), servers, network security appliances, and are not only export controlled, but when exported under license exception “ENC,” applicable semi-annual ENC reporting or annual self-classification reporting may also be required.

Where should you start to identify these exports? The most common encryption exports are non-revenue items, when your IT department exports equipment to support an operation, for example, or software is posted for download by a customer. As such, movement of items like this might not show up in your ERP system as an export.

However, this data may be stored elsewhere. Finance might track company assets in the ERP system, whereas downloads from support sites may be captured electronically. A shipping department would generate the shipment paperwork for physical exports, meaning that this may be the only place certain exports are recorded.

ERP, GTM and shipping systems for couriers should have some or most of the data required to generate the semi-annual ENC report. Search for shipments containing any items with an Export Control Classification Number (ECCN) of 5A002, 5D002 or 5E002.

Semi-annual reporting is required for exports to all destinations other than Canada, and for reexports from Canada for items described under Export Administration Regulations §740.17 (b)(2) and (b)(3)(ii). And there are exclusions.

Thus, it is not as simple as running an export report by ECCN, unless your company is also capturing the ENC citation. In addition, close reading is required to understand what the exact reporting requirements are, and what items fall under each ENC citation. In the past, there were general buckets referred to as “Restricted” and “Unrestricted” that helped with reporting, but those terms are history.

Annual self-classification reporting is required for items classified as ECCN 5A002, 5B002, or 5D002 described in §740.17 (b)(1) that do not have a CCATS and for Mass Market items classified as 5A992.c or 5D992.c under EAR Category 5 - Part 2 Note 3.

This is a lot of regulatory information to absorb, so we suggest that once you have searched your systems for the ECCN’s listed above, visit section §740.17 “Encryption Commodities, Software, and Technology” of the Export Administration Regulations (ENC) on the BIS website (www.bis.doc.gov). This will help you understand the requirements for using license exception ENC, and the reporting requirements.

It is important to note, however, that some regulatory changes impacting encryption reporting came into force on Sept. 20, 2016 and were not reflected in the policy guidance section of the BIS website. Understandably, this caused a great deal of confusion for companies preparing encryption reporting for Feb. 1, as firms had built reports to streamline the ENC reporting process, and some suddenly found they had to build new reports to account for the elimination of certain requirements and the expansion of others.

It may not be your direct responsibility, but if no one is preparing these encryption reports, you likely have a trade compliance gap. Government agencies are sharing information more than ever, and if they see you are exporting encryption items, but failing to submit the applicable reports, there may be negative consequences.

As this is may be a big undertaking, especially if not historically addressed, we recommend creating an ENC reporting team consisting of representatives from shipping/logistics, export, IT, customer support, engineering, marketing, sales, and finance to identify any revenue and non-revenue encryption exports (physical and download) and understand the reporting requirements. Retain external expertise to help you wade through the regulations and apply them to your export scenarios. Then develop policies and procedures to capture the required data, and automate reporting as much as possible.

The next ENC reporting deadline is Aug. 1. Will you be ready?

Roe is a director at BPE Global, a global trade consulting firm. She can reached by email at renee@bpeglobal.com.