Enforcement is Up! Time to Combat the Myths of Export Compliance

Have you heard the story about a policeman who stops a speeding car? The driver asks the policeman why they were stopped when other cars were clearly going faster. The policeman asks the driver "Have you ever gone fishing?" The driver nods. The policeman then asks, "Did you catch all the fish?" I think of this story every time I hear someone say: "There are bigger fish out there. Surely the government doesn't care about us!" While it's true there may be bigger fish out there, this doesn't mean that companies don't have to worry about the state of their compliance program, especially since the U.S. government is increasingly taking steps towards ramping up enforcement.

For example, last October, the Department of Commerce announced in a memo their enhanced enforcement of antiboycott rules, which included enhanced penalties, reprioritized violation categories, the requirement for parties entering into settlement agreements to admit misconduct, and a renewed focus on foreign subsidiaries of U.S. companies. Then, this past February the Department of Commerce and Department of Justice jointly launched the Disruptive Technologies Strike Force, whose purpose they have stated is to "counter efforts by hostile nation-states to illicitly acquire sensitive U.S. technology to advance their authoritarian regimes and facilitate human rights abuses." Within 3 months they had already announced criminal charges in 5 cases, and just last month they announced the issuance of a Temporary Denial Order suspending the export privileges of one of the individuals charged.

Considering this enhanced enforcement landscape, I thought it would be a good time to address some of the common "bigger fish" myths companies are sometimes led to believe, and how to address them before enforcement officers reel you in.

1. **We don't export to Russia or China, so we're OK.** With so much attention being given to Russia and China these days, one can easily be lulled into complacency and not worry as much about exports to other destinations. But other controls may apply, and violations are violations, regardless of the countries involved. Documented processes, and even better, systems, should account for the ECCN-based license requirements for all products to all destinations to which you export. Besides, even if you don't export to the most sensitive destinations, might you have a "deemed export" on your hands? Screening should nevertheless be conducted to ensure that those employees working on the company's most sensitive products and technologies in the U.S. are authorized to do so and do not require a license based on their most recent country of citizenship or permanent residency status. Finally, mechanisms should be considered to require a review in advance of any changes that could potentially introduce new customers or partners in, or who primarily do business in, these high visibility regions.

2. **We use great logistics providers, and they take care of all our export requirements.** While logistics providers offer a wide variety of services to help companies get their products exported, as the exporter, your company is still liable in the event of any violation. If they're classifying products on your behalf, those classifications should be reviewed on a regular basis for accuracy. If you haven't already done so, request that they provide you with soft copies of all documents for audit and recordkeeping purposes. Any required reporting, such as that of Electronic Export Information data elements, should be regularly screened to confirm it matches your commercial invoice. Reports

available to your company through CBP's ACE Secure Data Portal would be highly useful for this screening. Then, companies should also confirm that the products are getting to their intended destination. As we often say in the field of compliance, "Trust, but verify."

3. **We operate under a distribution/reseller model, and we don't need to have visibility for end-users.** Not knowing who the end users of your products are, or not knowing their intended end use, could lead to your company's products ending up in the hands of restricted parties, or being used in restricted Weapons of Mass Destruction applications. At minimum, distributors and resellers should be required to sign a statement of compliance with export control laws, and to recertify on an annual cadence to account for any changes in staff or business model. If new to your company, they should undergo a thorough assessment to ensure there is no risk of your company's products being diverted for illicit use. If parts are shipped back to you directly from end users for repair or replacement, conduct a restricted party screening on them as you would for a new customer before you re-export to them.

4. **We have an Export Compliance Program Manual and can use that as a mitigating factor in the event of a violation.** While that may be true, it would only help if you're doing what it says. Review your manual on an annual basis to ensure corresponding procedures haven't changed, and to be certain that all compliance requirements are addressed. For example, although they aren't often discussed, last October's memo, coupled with recent penalties of $283,500 assessed against Regal Benoit for Antiboycott Regulations tells us the Department of Commerce cares about those rules. Do you? Plus, remember that export compliance involves more agencies than just the Department of Commerce. Does your compliance program include screening for compliance with OFAC sanctions programs, including their 50% rule? Any company directly or indirectly majority-owned (in aggregate) by blocked parties is also effectively blocked. Therefore, you may be prohibited from doing business with them even if they don't appear on an OFAC list.

5. **We don't make disruptive technologies. Our products are all EAR99.** I agree, we all love EAR99. But don't forget that EAR99 products are still subject to the EAR, and therefore still subject to the 10 General Prohibitions. The Department of Commerce is also tasked with identifying sensitive technologies to the United States and if your products are cutting edge, or have sensitive applications, you may benefit from seeking guidance before casually assigning them an EAR99 classification. Of equal importance, if you're using controlled equipment or materials to manufacture that EAR99 product, your company should still have a technology control plan in place to ensure no inadvertent violations of the deemed export rule occur (yes, there's that rule again!)

Whether it be restricted parties screening, filing export data, auditing records, classifying products and considering their export license implications , creating procedures, or building systems to automate compliance, there is always work to be done. If you've recently found yourself making any of the above statements, and need the support to bolster your compliance program, we're here for you. Let BPE Global know if we can help you with any of your trade compliance needs. BPE Global is a global trade consulting and training firm. Evelyn Bernal is a Director of BPE Global. You can reach Evelyn by email at ebernal@bpeglobal.com or by phone at 408-718-0265.