Key Export Compliance Issues For 2016

02.10.2016

The following are a number of important strategic issues to be considered in the export compliance area for the new year.

1. Recent Country Amendments – New Obligations and New Opportunities. There have been export law amendments affecting a large number of countries within the past year – including Cuba, Iran, Burma, N. Korea, Crimea, Burundi, Belarus, Liberia, Venezuela and Russia, among others. These present additional obligations in some countries and opportunities in others. Exporters should update their compliance programs to reflect these changes – and for some countries and products (such as Cuba, aircraft parts, pistachios and General License H) update their business plans as well. If you do not have a compliance program this is the first order of business - you should address this right away.

2. Update Export Classifications. The foundation of an export compliance effort is determining the export jurisdiction and classification of your products and services – this is the critical first step in identifying the export requirements that will apply to your company. There have been significant amendments to the U.S. Munitions List and the Commerce Control List over the past eighteen months under Export Control Reform ("ECR"). Now that ECR is winding down, you should be sure that your export classifications are up to date and reflect these changes. As the saying goes – garbage in, garbage out – if the classifications are incorrect the entire rest of the program may be defective.

3. Cybersecurity and Export Violations. One of the most significant issues exporters will face in the upcoming year is the risk of export control liability for cybersecurity breaches. The Bureau of Industry and Security ("BIS") and the Directorate of Defense Trade Controls ("DDTC") are expected to issue final regulations shortly regarding data security standards in using "end-to-end encryption" in the revised definition of "export" under proposed 15 CFR §§734.13 and 734.18(a)(4) and 22 CFR §§ 120.17 and 120.52(a)(4), and may issue additional pronouncements regarding other cyber security obligations of exporters.[1] The Department of Defense has also issued amendments to the Defense Federal Acquisition Regulation Supplement (DFARS) addressing data security standards for government contractors, including the handling of ITAR-controlled and EAR-controlled data as "covered defense information."[2] If a company experiences a cyber-intrusion and ITAR-controlled

technical data or EAR-controlled technology are compromised, the company risks serious liability unless it has the proper level of data security controls deployed in its network. Pay close attention to developments in this area in coming months.

4. High Risk Transactions. One tried-and-true compliance strategy could be the most valuable best practice for 2016 - have a process for identifying and avoiding high-risk transactions. This is particularly important in light of the fast pace of recent changes in export restrictions and sanctions designations due to terrorist, nuclear and military actions worldwide. One of the greatest risks for U.S. exporters is the risk of unauthorized diversion/transshipment – you sell your product to one party, and that party without your knowledge resells your product to a prohibited country, prohibited party or for a prohibited end use. BIS enforcement officials have stated that *the majority of export enforcement cases are now for EAR99 violations – this means products going to prohibited countries, prohibited parties or used for prohibited end uses*. You should upgrade your compliance processes to identify high risk transactions, including high risk countries, parties, industries/products, transshipment hubs, unsavory business practices and red flag indicators. Once identified, use enhanced compliance steps to reduce risk, or avoid these transactions completely.

5. Personal Liability For Export Violations. The September 9, 2015 Memorandum by Deputy Attorney General Sally Quillian Yates sent a chilling message to the business community – federal prosecutors will be looking to increase prosecution of individual defendants in corporate enforcement cases. This will surely apply to violations under sanctions laws, defense trade controls and BIS export controls. We are not sure if this is a passing political trend or a serious shift in law enforcement strategy, however exporters are advised to take this seriously in planning the scope and rigor of their export compliance efforts.

The new year brings new opportunities and challenges for export compliance professionals. With the proper planning and the right execution, your company can remain safe and prosper in the year ahead.

[1] See Proposed Rule, Department of Commerce, Bureau of Industry and Security, Revisions to Definitions in the Export Administration Regulations, Federal Register Vol. 80, No. 106, June 3, 2015, p.31505 et. seq., and Proposed Rule, Department of State, International Traffic in Arms: Revisions to Definitions of Defense Services, Technical Data, and Public Domain; Definition of Product of Fundamental Research; Electronic Transmission and Storage of Technical Data; and Related Definitions, Federal Register Vol. 80, No. 106, June 3, 2015, p.31525 et. seq.

\[2] See Interim Rule, Department of Defense, Defense Acquisition Regulations System, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Federal Register Vol. 80, pp 51739 et. Seq., August 26, 2015 and See Interim Rule,

Department of Defense, Defense Acquisition Regulations System, Defense Federal Acquisition Regulation Supplement: Network Penetration Reporting and Contracting for Cloud Services (DFARS Case 2013-D018), Federal Register Vol. 80, pp 81472, et seq., December 30, 2015.

Related People

- Thomas B. McVey – 202.293.8118 – tmcvey@williamsmullen.com

Related Services

- ITAR, Export Controls and Economic Sanctions
- International
- Government Contracts