



## Company Incurs \$6 Million Penalty for Export of Controlled Software and Technical Data

09.20.2021

A recent export enforcement case describes a common compliance challenge faced by many U.S. companies. In this case,[1] a California company manufactured electronic test and measurement equipment for both commercial and government customers. The company failed to identify that one of its software products was listed on the U.S. Munitions List and subject to ITAR. It then exported the software to seventeen countries, including Canada, Australia, France, Germany, Japan, Israel, Russia and China without an export license. The Directorate of Defense Trade Controls (DDTC) determined that the software was controlled under USML Category XI(d) and brought an enforcement case alleging 24 ITAR violations, resulting in a \$6,600,000 penalty for the company.[2]

In addition to the monetary penalty, DDTC imposed a litany of remedial measures on the company including the requirement to hire a compliance monitor, adopt enhanced compliance procedures and conduct a detailed classification review and an export compliance audit. The Consent Agreement also provided that, if the company is acquired in the future through a merger or acquisition, the purchaser acquiring the company will become subject to those remedial measures.

DDTC recognized the possibility that the company's violations were inadvertent ? in its Charging Letter DDTC stated: ?Respondent claims that these exports were based on a good faith but misguided belief that the MESG software was not subject to ITAR.[3] Yet DDTC proceeded with the enforcement case anyway. Enforcement agencies can bring civil enforcement actions even if they believe the companies were not aware of the legal requirements that applied and the violations were unintentional. If DDTC determined that the violations were *intentional* it could have referred the case for criminal prosecution with much higher criminal penalties - up to \$1,000,000 or 20 years imprisonment, or both, per violation.

Copies are available here of the DDTC Charging Letter, Consent Agreement and Order in this case.

This is an all-too-common scenario - companies without export compliance resources can unintentionally overlook requirements under the International Traffic In Arms Regulations (ITAR) and the Export Administration Regulations (EAR). Companies that operate full time in the defense sector most

likely have detailed export compliance procedures. However companies in the commercial sector, with no or few government customers, frequently are not aware of these requirements, such as licensing, data controls and controls on "defense services." Similarly, such companies may not recognize that export control requirements apply not just to physical products but also to technical data and software as well, and companies are prohibited from disclosing controlled technical data and software to foreign nationals abroad or in the U.S. (including to the company's foreign national employees.) Such companies may even be selling to commercial customers without knowledge that the customers will be reselling the products for eventual use in defense end-products.

*Even if a product is not used in the defense sector, many commercial products are subject to export restrictions under the Export Administration Regulations which apply to a broad array of purely commercial products.*

Such companies can be at risk for committing significant export violations, even if they are not aware of these requirements or incorrectly interpret them. Requirements can arise in many industries, including electronics, computers and software, communications, general manufacturing, engineering/technical services, chemical, marine, aerospace, avionics, security, advanced materials, UAVs, space/satellites and many more. These problems occur throughout the entire supply chain, down to the lowest level of suppliers and service providers.

However there are a number of steps that companies can take to become savvy in export compliance and to reduce these risks ? they include:

- Reviewing your products and services to determine if they are listed on the U.S. Munitions List (USML) or the Commerce Control List (CCL) and may be subject to ITAR or EAR requirements;
- Based on this review, identifying the legal requirements that may apply to your company in its current business operations;<sup>[4]</sup>
- If required, registering with the State Department under ITAR §122.1;
- Recognizing that controls apply not just to physical products but also to technical data and software, and may apply to "defense services" under ITAR Part 124;
- Using care not to disclose controlled technical information or software to foreign nationals in the U.S. if such disclosure requires a license, including to foreign national employees of your company;
- Adopting controls in your company's data system to prevent unauthorized persons (including foreign national employees in your company) from having access to controlled technology and software stored in your data system;
- Adopting an Export Compliance Program to identify written procedures within your company to comply with these requirements and providing export compliance training for employees who are involved in activities under ITAR and EAR; and
- Conducting this review not just for existing products but for new products, contracts etc. that the company becomes involved with in the future as part of its normal business process.

For a detailed list of a number of the requirements under ITAR we recommend reviewing [ITAR For Government Contractors and ITAR Compliance Checklist](#).

The Keysight Technologies case discussed above is not the only enforcement case involving companies that operate in the commercial sector ? there are many other examples of such cases<sup>[5]</sup>

It is well known that many companies in the government contracts/defense sectors are subject to requirements under the ITAR or EAR. However, companies that operate in the commercial sector can also have responsibilities under these laws. It is important for companies in commercial industries to understand these requirements and how they apply to them. A bit of caution and foresight may save the company significant legal disruption in the future ? and a \$6 million penalty.

For additional resources for small and mid-sized government contractors and suppliers on ITAR compliance please see:

- [Understanding the OFAC Sanctions Laws](#)
- [Avalanche of Recent Export Requirements for China, Russia And Other Countries](#)
- [Dealing with Violations in Export and Import Transactions](#)

To learn about how Williams Mullen can assist your company in ITAR compliance, please click [here](#).

Please note: This article contains general, condensed summaries of actual legal matters, statutes and opinions for information purposes. It is not meant to be and should not be construed as legal advice. Readers with particular needs on specific issues should retain the services of competent counsel. For more information, please visit our website at [www.williamsmullen.com](http://www.williamsmullen.com) or contact Thomas B. McVey, 202.293.8118 or [tmcvey@williamsmullen.com](mailto:tmcvey@williamsmullen.com).

[1] See [In the Matter of Keysight Technologies, Inc. Proposed Charging Letter, Consent Agreement and Order](#), available on the Directorate of Defense Trade Controls website.

[2] See [Keysight Technologies Consent Agreement](#) cited above.

[3] See [Keysight Technologies Charging Letter](#) cited above, p. 3.

[4] Such requirements under ITAR include licensing for exports, reexports and temporary imports of ITAR-controlled items, registration, requirement to obtain Technical Assistance Agreements (TAAs) for the performance of ?defense services,? authorizations for the licensing of the manufacture or distribution of ITAR-controlled products overseas, controls on the export and domestic disclosure to foreign nationals of controlled technical data and software,

requirements on the "brokering" of ITAR-controlled items, requirements to file reports under ITAR Part 130, restrictions on transactions with debarred parties and recordkeeping requirements. The EAR have similar but, in certain cases, different requirements. [5] See, for example, cases involving Darling Industries, Inc., Microwave Engineering Co., and Rocky Mountain Instrument Company available on the DDTC website.

## **Related People**

- Christopher H. Skinner ? 202.293.8129 ? cskinner@williamsmullen.com

## **Related Services**

- ITAR, Export Controls and Economic Sanctions