TORRES LAW

INTERNATIONAL TRADE & NATIONAL SECURITY

Noteworthy ITAR Enforcement Actions in 2021

January 2022 | Torres Law, PLLC

***

Torres Law, PLLC is an international trade and national security law firm that assists clients with the import and export of goods, technology, and services. The firm has extensive experience with the various regimes and agencies governing trade such as the Directorate of Defense Trade Controls, the Bureau of Industry and Security, the Office of Foreign Assets Control, the U.S. Customs and Border Protection, and others. Our group provides clients with full support for all trade law issues, including U.S. export control and sanctions laws, industrial security, the Foreign Corrupt Practices Act, anti-boycott laws, and customs laws.

ABOUT TORRES LAW

Torres Law is an international trade and national security law firm that assists clients with the import and export of goods, technology, and services. We have extensive experience with the various regimes and agencies governing national security and trade such as U.S. Customs and Border Protection, the Department of Commerce Bureau of Industry and Security, the Department of State Directorate of Defense Trade Controls, the Department of Treasury Office of Foreign Assets Control, the Committee on Foreign Investment in the United States, the Defense Counterintelligence and Security Agency and others. Our group provides clients with full support for all trade and national security law issues, including U.S. export control and economic sanctions laws, industrial security, and trade strategy and policy.

Global Law Experts 2021 Annual Awards Winner

Ranked in Chambers USA 2021 – Olga Torres

Rated by Super Lawyers

Proud Member of AlliottGlobalAlliance

International Lawyers Network

PRACTICE AREAS

CUSTOMS
U.S. Customs and Border Protection, Border Compliance and EU Customs

EXPORTS
International Traffic in Arms Regulations, Export Administration Regulations, Foreign Trade Regulations Census, and EU Export Controls

ECONOMIC SANCTIONS
Office of Foreign Assets Control (OFAC) and EU Embargoes

FCPA
US and foreign country anti-corruption laws

INDUSTRIAL SECURITY
Committee on foreign investment the US (CFIUS) and Foreign Ownership, Control, or Influence (FOCI)

www.torrestradelaw.com

CONTACT US BY EMAIL AT
info@torrestradelaw.com

TORRES LAW
INTERNATIONAL TRADE & NATIONAL SECURITY

Noteworthy ITAR Enforcement Actions in 2021

The U.S. Department of State ("State Department") is responsible for the export and temporary import of defense articles and services governed by the Arms Export Control Act ("AECA")[1] and Executive Order 13637 ("E.O. 13637")[2]. The International Traffic in Arms Regulations ("ITAR"),[3] which implements the AECA, is administered by the Directorate of Defense Trade Controls ("DDTC") in the Bureau of Political-Military Affairs at the State Department. The DDTC is tasked with protecting U.S. national security by restricting and controlling the manufacture, sale, and distribution of defense and military items and services.

DDTC publishes copies of final settlement documents for ITAR administrative actions, including charging letters, consent agreements, and orders. Since 1978, the DDTC has published documents for 64 dated actions. There is an average of two DDTC actions per year and no year saw more than five DDTC actions. Certain companies, including Boeing, Lockheed Martin, L-3, Raytheon, ITT, Hughes and Security Assistance International, have been penalized more than twice. DDTC only brought two enforcement actions in 2021.

***

Keysight Technologies, Inc.

On August 3, 2021, DDTC ordered that Keysight Technologies, Inc. ("Keysight"), a defense contractor located in North Carolina, pay in fines and in remedial compliance measures a civil penalty of $6,600,000, in complete settlement of its potential liability resulting from 24 apparent violations of section 127.1(a)(1) (unauthorized exports of technical data) of the ITAR.

Specifically, the 24 apparent violations are the result of Keysight's unauthorized export of technical data, including software, controlled under USML Category XI(d) to Australia, Canada, China, Czech Republic, France, Germany, India, Israel, Japan, Russia, Singapore, South Korea, Spain, Switzerland, Taiwan, Turkey, and the United Kingdom. Moreover, 13 of the 24 charges involve unauthorized exports to China, a proscribed destination pursuant to section 126.1 of the ITAR; and two of the 24 charges involve unauthorized exports to Russia, also a proscribed destination for defense exports.

Keysight's Unauthorized Exports of Technical Data, Including Software, to Multiple Countries

On November 9, 2017, the Office of Defense Controls Trade Policy ("DCTP") raised concern over Keysight's potential misclassification of its Signal Studio for Multi-Emitter Scenario Generation software ("MESG software") and recommended Keysight submit a commodity jurisdiction ("CJ") request to determine the jurisdiction of the software.

Between 2015 and 2018, Keysight exported its MESG software in two forms: full versions of the software installed on hardware or electronically and trial versions of the software via downloads from their website.

[1] Arms Export Control Act, 22 U.S.C. §§ 2751–2799aa-2.
[2] Administration of Reformed Export Controls, Exec. Order No. 13,637, 78 Fed. Reg. 16,127 (Mar. 13, 2013).
[3] International Traffic in Arms Regulations, 22 C.F.R. §§ 120–130 (2021).

On January 4, 2018, in response to DCTP's recommendation, Keysight submitted a CJ request to State. Between January 9, 2018, and April 18, 2018, while its CJ request was under review, Keysight continued to export its MESG software on eight separate occasions to China, Russia, Japan, Israel, and Canada. On April 27, 2018, DDTC provided Keysight with a determination that the MESG software was controlled under USML Category XI(d) due to the software's direct relation to electronic warfare test sets described by USML Category XI(a)(11). Following this formal determination, Keysight ceased any further unlicensed exports of MESG software and began treating MESG software as ITAR-controlled. On April 30, 2018, Keysight appealed the CJ determination by submitting a reconsideration request, which was subsequently reaffirmed.

On May 21, 2018, Keysight submitted an initial disclosure and later, on July 24, 2018, submitted a full disclosure, revealing the unauthorized export to multiple countries of its MESG software, which Keysight had self-determined was subject to the EAR and controlled as EAR99. Following Keysight's submission of its full disclosure, the U.S. Government reviewed Keysight's actions and assessed that Keysight's exports to China and Russia harmed U.S. national security.

Aggravating Factors

(1) Certain violations harmed U.S. national security;
(2) Certain violations involved unauthorized exports to China;
(3) Certain violations involved unauthorized exports to Russia;
(4) State notified Keysight of misclassifications concerns, which led to the discovery of ITAR violations; and
(5) Keysight continued exporting the MESG software as EAR99 while the CJ request was under review.

Mitigating Factors

(1) Keysight cooperated with State's review of the potential violations and submitted a disclosure acknowledging the charged conduct after State alerted Keysight of misclassification concerns.
(2) Keysight implemented remedial compliance measures intended to detect, deter, and prevent future similar violations.
(3) Keysight cooperated and entered into an agreement with the DDTC tolling the statutory period that applies to enforcement of the AECA and the ITAR.

Honeywell International, Inc.

On April 27, 2021, DDTC ordered that Honeywell, a Delaware-based conglomerate involved in the aerospace, building technology, performance material, and safety solution industries, be assessed a civil penalty in the amount of $13,000,000 per the terms of a consent agreement with Honeywell for 34 violations of section 127.1(a)(1) (unauthorized exports and retransfers of technical data) of the ITAR. DDTC determined not to impose an administrative debarment of Honeywell.

The 34 ITAR violations are derived from Honeywell's two voluntary disclosures of its unauthorized exports and retransfers of ITAR-controlled drawings and technical data to Canada,

Ireland, Mexico, China, and Taiwan between July 2011 and October 2015, and between June and July of 2018.

Honeywell's Unauthorized Exports and Retransfers from July 2011 to October 2015
In December 2015, Honeywell disclosed to the DDTC that Honeywell's Aerospace business group's Integrated Supply Chain ("ISC") organization had, in July 2015, exported without authorization multiple ITAR-controlled drawings to suppliers in Taiwan and China through a file exchange platform, DEXcenter. The drawings were sent as Requests for Quotations ("RFQ") to the suppliers. Upon DDTC's request, Honeywell ultimately identified that 71 ITAR-controlled drawings had been exported between July 2011 and October 2015 without authorization via DEXcenter to Canada, Ireland, China, and Taiwan.

The 71 drawings were controlled under USML Categories VIII(i), XI(d), and XIX(g). The drawings contained engineering prints showing layouts, dimensions, and geometries for manufacturing castings and finished parts for aircrafts, military electronics, and gas turbine engines, including the F-35, F-22, T55 turboshaft engine, among others. Some of the drawings contained technical data designated as Significant Military Equipment ("SME").

Honeywell exported 51 of the 71 drawings to suppliers in China, a proscribed destination under ITAR § 126.1(d)(1). Honeywell also exported 20 of the 71 drawings to its subsidiaries in China, and the subsidiaries then retransferred 16 drawings to unaffiliated suppliers in China. The U.S. Government determined that these exports to, and retransfers in, China, specifically those of drawings for certain parts and components for the engine platforms for the F-35 Joint Strike Fighter, B-1B Lancer Long-Range Strategic Bomber, and the F-22 Fighter Aircraft, harmed U.S. national security.

Honeywell's Unauthorized Exports and Retransfers of Technical Data in 2018 Despite Purported Implementation of Corrective Actions in 2016
In its September 2016 full voluntary disclosure, Honeywell notified DDTC of multiple corrective actions it had taken to prevent the types of violations it disclosed. The actions included:

1. A mandatory second-level review requirement for all international document transfers through DEXcenter;
2. Mandatory training measures to address the risk of human error due to misidentifying export classification or authorizations, especially in the RFQ context; and
3. Enhancing DEXcenter to further reduce the risk of human error by:
    a. Limiting the user's ability to select an export authorization that does not match a drawing's export classification; and
    b. Providing additional warnings, reminders, and training resources and requirements.

In October 2018, Honeywell submitted a second voluntary disclosure describing how ISC personnel committed another series of ITAR violations. Specifically, Honeywell disclosed that a team of U.S. ISC personnel implemented a new export compliance process for soliciting RFQs that either failed to review the export control classifications for multiple technical documents or used a classification analysis method that did not properly categorize the documents as described on either the USML or the CCL.

Between June and July of 2018, and under the new export compliance process, ISC personnel exported 27 ITAR-controlled drawings without authorization to Canada, China, and Mexico. The drawings were controlled under USML Categories VIII(i) and XIX(g), contained engineering prints showing layouts, dimensions, and geometries for manufacturing castings and finished parts for aircraft and gas turbine engines, including the F-35, T55 turboshaft engine, and the CTS800 turboshaft engine, among others. Some of the drawings contained technical data described as SME pursuant to ITAR § 121.1(a)(2).

Honeywell exported two drawings to an employee of one of its subsidiaries in China, which is a proscribed destination under ITAR § 126.1(d)(1). Honeywell also disclosed that this employee retransferred one of the two drawings to another employee at its subsidiary in China.

The USG reviewed copies of the 23 drawings and determined that the exports to and retransfers in China of drawings for certain parts and components of the CTS800 gas turbine engine undermined U.S. national security.

TORRES LAW

INTERNATIONAL TRADE & NATIONAL SECURITY

Questions? Contact Us:

Call 202.851.8200 or 214.295.8473
Email Info@torrestradelaw.com

Sign up for our newsletter: www.torrestradelaw.com