



# Don't Let This **HAPPEN** **TO YOU!**



Actual Investigations *of*  
Export Control *and*  
Antiboycott Violations

SEPTEMBER 2019



U.S. DEPARTMENT OF COMMERCE  
Bureau of Industry and Security  
Export Enforcement

**DON'T LET THIS HAPPEN TO YOU!!!**

## **An Introduction to the Consequences of Violating U.S. Export Control Law**

*Actual Investigations of Export Control and Antiboycott Violations*



SEPTEMBER 2019

**EXPORT ENFORCEMENT**

BUREAU OF INDUSTRY AND SECURITY  
U.S. DEPARTMENT OF COMMERCE

## Summary Table of Contents

<b>Introduction</b>	Page 2
<b>Mission and Organization</b>	Page 2
Office of Export Enforcement	Page 3
Office of Enforcement Analysis	Page 5
Office of Antiboycott Compliance	Page 6
<b>Authorities and Remedies</b>	Page 6
Criminal and Civil Penalties	Page 6
Voluntary Self-Disclosures	Page 8
Denial of Export Privileges	Page 9
BIS-Administered Lists	Page 9
Asset Forfeiture	Page 10
False Statements	Page 11
<b>Export Compliance</b>	Page 11
Responsible Parties	Page 11
Eight Principles for an Effective Compliance Program	Page 11
Transshipments & Reexports	Page 13
Catch-All Controls	Page 13
Successor Liability	Page 14
Educational Outreach	Page 14
Cyber-Intrusions and Data Exfiltration	Page 15

## Chapter 1 – Terrorism and State Sponsors of Terrorism

<b>Introduction</b>	Page 16
<b>Criminal and Administrative Case Examples</b>	Page 17
David Levick / ICM Components	Page 17
Arash Sepehri / Tajhiz Sanat Shayan	Page 17
Arzu Sagsoz / Kral Havacilik	Page 18
Ali Caby / Marjan Caby / Arash Caby	Page 18
Ali Eslamian	Page 18
Worthington Products, Inc. / Hydrel Engineering Products	Page 19
Hassan Zafari	Page 19
Erdal Akova / Esa Kimya	Page 20
Mansour Zadeh	Page 20
National Oilwell Varco / Dreco Energy Services Ltd.	Page 20
Tayabi Fazal Hussain / Prime PE International Trading Company	Page 20
Harold Rinko / Ahmed Feras Deri / Global Parts Supply	Page 21
Technoline SAL / Berty Tyloo	Page 21
Fokker Services B.V.	Page 22
Amin Al-Baroudi	Page 22
Oguzhan Aydin	Page 22
Ali Reza Parsa / Metal PM	Page 23
Sihai Cheng	Page 23
Corezing International Pte, Ltd.	Page 24
Antennas and Components / Eric Schneider	Page 24

Springworks Sdn Bhd / Kenneth Chua / Owen Chen .....	Page 25
Barracuda Networks, Inc. and Barracuda Networks Ltd .....	Page 25
EgyptAir Airlines Company.....	Page 25
Mozaffar Khazaee .....	Page 26
Schlumberger Oilfield Holdings Ltd. ....	Page 26
Borna “Brad” Faizy / Touraj Ghavidel / Techonweb.....	Page 27
Hetran, Inc. / Helmut Oertmann / FIMCO FZE .....	Page 27
Ya Qian “Jonathan” Chen / SKS Hydraulics USA, Inc. ....	Page 28
Trans Merits Co., Ltd. ....	Page 28
Mohammad Reza Hajian / RH International LLC / Nexiant LLC / P & P Computers LLC / Randy Barber / Michael Dragoni / Fortis Data Systems LLC / Greencloud LLC / John Talley / Tallyho Peripherals, Inc....	Page 28
Computerlinks FZCO / Infotec / Waseem Jawad / Aramex Emirates LLC .....	Page 29
Weatherford International .....	Page 30
Mahan Airways and Balli Group PLC .....	Page 30
Mohammad Tabibi / Michael Edward Todd / Hamid Seifi / Parts Guys LLC / Galaxy Aviation Services .....	Page 31
Mayrow General Trading Network.....	Page 32

## Chapter 2 – Commerce Control List

Introduction .....	Page 33
<b>Criminal and Administrative Case Examples</b> .....	Page 34
<i>Nuclear Nonproliferation Controls</i>	
Imran Khan / Kamran Khan / Muhammad Ismail .....	Page 34
MHz Electronics, Inc. ....	Page 34
Fuyi Sun / Zhong Li Bang Ye International Trading Co. Ltd.....	Page 34
Cryofab, Inc. ....	Page 35
Trexim Corporation / Bilal Ahmed .....	Page 35
Teledyne LeCroy .....	Page 35
Nicholas Kaiga / IMC Metals Company .....	Page 36
Qiang (Johnson) Hu / MKS Shanghai.....	Page 36



Lisong Ma.....	Page 36
Xun Wang / PPG Paints Trading (Shanghai) Co., Ltd. / Huaxing Construction.....	Page 37
Nadeem Akhtar / Computer Communication USA.....	Page 37
Jirair Avanessian / Farhad Masoumian Amirhossein Sairafi / XVAC.....	Page 38
Peter Gromacki / Hamid Reza Hashemi/ Amir Abbas Tamimi / Murat Taskiran....	Page 38
<b><i>Chemical/Biological Weapons Controls</i></b> .....	Page 39
Envirotech Pump Systems, Inc.....	Page 39
Flowserve Corporation.....	Page 39
Buehler Limited.....	Page 39
Dr. Thomas Butler.....	Page 40
<b><i>Missile Technology Controls</i></b> .....	Page 41
Erdal Kuyumcu / Global Metallurgy.....	Page 41
Weiss Envirotronics .....	Page 41
C.A. Litzler Co., Inc.....	Page 41
Ming Suan Zhang.....	Page 42
GrafTech International Holdings .....	Page 42
Parthasarathy Sudarshan / Mythili Gopal / Cirrus Electronics LLC .....	Page 42
<b><i>National Security Controls</i></b> .....	Page 43
Zhongxing Telecommunications Equipment Corporation (ZTE) and ZTE Kangxun Telecommunications Equipment.....	Page 43
Peter Zuccarelli / Sayed Razvi / American Coating Technologies .....	Page 43
Si Chen / Archangel Systems Space .....	Page 44
Bryan Singer.....	Page 44
Arc Electronics / Alexander Fishenko / Alexander Posobilov / Shavkat Abdullaev / Anastasia Diatlova.....	Page 45
Seiler Instruments & Manufacturing Co. ....	Page 45
Alexy Barysheff / Alexy Krutinin / Dimitri Karpenko .....	Page 45
Millitech, Inc. ....	Page 46
Saied Charkhian / Caspian Industrial Machinery Supply LLC .....	Page 46
Alexander Brazhnikov / ABN Universal.....	Page 46
Daofu Zhang / Jian Guanghou Yan / Xianfeng Zuo.....	Page 47
Unisol .....	Page 47
Mark Henry .....	Page 47
Streit USA Armoring LLC / Streit Middle East / Streit Group FZE / Guerman Goutorov / Eric Carlson .....	Page 48
Zhenchun “Ted” Huang .....	Page 49
Zhen Zhou Wu / Yufeng Wei /Bo Li / Chitron Electronics, Inc. ....	Page 49
Timothy Gormley / Amplifier Research Corporation .....	Page 49
<b><i>Crime Controls</i></b> .....	Page 50
Patrick Germain.....	Page 50
Rasheed Al Jijakli / Palmyra Corporation.....	Page 50
Kenneth Chait / Tubeman.com/Advantage Tube Services, Inc. ....	Page 51
Dmytro Medvedyev.....	Page 51
Shehzad John.....	Page 51
Kan Chen.....	Page 52

Hassan Salame.....	Page 52
B&H Foto & Electronics Corp.....	Page 53
Mike Cabatingan / Romulo Reclusado.....	Page 53
Lev Steinberg .....	Page 53
Vitali Tsishuk / Volha Dubouskaya / Aliaksandr Stashynski / Yahor Osin / Aliaksandr Belski / Ernest Chornoletsky .....	Page 53
Mark Komoroski / Sergey Korznikov / D&R Sports Center .....	Page 54

## Chapter 3 – Freight Forwarders

<b>Introduction</b> .....	Page 55
<b>Criminal and Administrative Case Examples</b> .....	Page 55
Eric Baird / Access USA Shipping, LLC .....	Page 55
Mohawk Global Logistics Corp. / Multiwire Laboratories .....	Page 56
Gennadiy Boyko / SHOPOZZ, Inc.....	Page 56
Federal Express .....	Page 57
Pilot Air Freight.....	Page 57
Asim Fareed / Compass Logistics International.....	Page 58
Fulfill Your Package .....	Page 58
General Logistics International .....	Page 59
Kintetsu World Express.....	Page 59
Rukhsana Kadri / R&A International Trading, Inc. ....	Page 59

## Chapter 4 – Deemed Exports

<b>Introduction</b> .....	Page 61
<b>Criminal and Administrative Case Examples</b> .....	Page 61
Intevac, Inc. ....	Page 61
Atmospheric Glow Technologies / J. Reece Roth.....	Page 61
Maxim Integrated Products, Inc. ....	Page 62
Ingersoll Machine Tools.....	Page 62
TFC Manufacturing, Inc. ....	Page 62

## Chapter 5 – Antiboycott Violations

<b>Introduction</b> .....	Page 63
<b>Criminal and Administrative Case Examples</b> .....	Page 64
RHDC International LLC .....	Page 64

Vinmar International, Ltd. / Vinmar Overseas, Ltd. ....	Page 65
Baker Eastern, SA (Libya) .....	Page 65
TMX Shipping Company, Inc.....	Page 65
Laptop Plaza, Inc. (aka IWEBMASTER NET, Inc.) .....	Page 66
Leprino Foods Company.....	Page 66
AIX Global LLC .....	Page 66

# SECURING AMERICA'S TRADE

1982 30 YEARS 2012



OFFICE OF EXPORT ENFORCEMENT  
BUREAU OF INDUSTRY AND SECURITY



U.S. DEPARTMENT OF COMMERCE





# Introduction to Enforcement of U.S. Export Controls

## Mission and Organization

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) administers and enforces export controls on dual-use and certain munitions items for the Department of Commerce through the Export Administration Regulations (EAR) under the authority of the Export Control Reform Act of 2018 (ECRA)<sup>1</sup>. Dual-use items are commodities, software, or technology that have both commercial and military or proliferation applications. Some examples of dual-use items may include things such as: smoke bombs, spiked batons, certain shotguns, shotgun shells and buckshot, rocket fuels, space launch vehicles, radiation hardened integrated circuits, turbines for use in nuclear reactors, integrated navigation systems designed or modified for use in missiles, chemical warfare precursors, biological containment facilities, radio frequency modules, triggered spark gaps, and carbon fiber. Controlled items listed under 600 series Export Control Classification Numbers (ECCN) are enumerated on the Commerce Control List (CCL) because they are items on the Wassenaar Arrangement Munitions List (WAML) or were formerly on the U.S. Munitions List (USML). Certain munitions items may include commodities, software, and/or technology such as military flight instrument trainers, lightweight turbojet engines, medical facilities for surface or submersible vessels of war, demolition blocks and detonators for military explosives, thrust or combustion chambers, armor plate for hard body armor, discrete microwave transistors, military concealment and deception equipment, smoke or obscuration equipment and simulators, submarine or torpedo nets, rebreathing apparatus specially designed for military use, submersible military vessels, thermal batteries, and telecommunications equipment for a military application.

Other federal agencies with a role in administering U.S. export controls include the Department of State, which controls the export of defense articles and defense services subject to the International Traffic in Arms Regulations (ITAR), the Department of Energy, which controls exports and reexports of technology related to the production of special nuclear materials, the Nuclear Regulatory Commission, which controls the export of certain nuclear materials and equipment, and the Department of the Treasury, which administers economic sanctions programs.

The Export Enforcement arm of BIS protects and promotes U.S. national security, foreign policy and economic interests by investigating violations, interdicting illegal exports, conducting end-use checks, educating parties to export transactions on how to improve export compliance practices and identify suspicious inquiries, supporting the licensing process by evaluating the bona fides of transaction parties, and

---

<sup>1</sup>The Export Administration Regulations originally issued pursuant to the Export Administration Act (50 U.S.C. §§ 4601-4623 (Supp. III 2015)) (EAA). On August 21, 2001, the EAA lapsed and the President, through Executive Order 13222 of August 17, 2001 (3 C.F.R., 2001 Comp. 783 (2002)), which was extended by successive Presidential Notices, the most recent being that of August 14, 2019 (84 Fed. Reg. 41, 881 (Aug. 15, 2019)), continued the Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. § 1701, et seq. (2012)) (IEEPA). On August 13, 2018, the President signed into law the John S. McCain National Defense Authorization Act for Fiscal Year 2019, which includes the Export Control Reform Act of 2018, 50 U.S.C. §§ 4801-4852 (ECRA).

Section 1768 of ECRA provides, in pertinent part, that all rules and regulations that were made or issued under the EAA, including as continued in effect pursuant to IEEPA, and were in effect as of ECRA's date of enactment (August 13, 2018), shall continue in effect until modified, superseded, set aside, or revoked through action undertaken pursuant to the authority provided under ECRA.

aggressively pursuing violators of export control laws for criminal prosecution or administrative penalties. BIS Export Enforcement has evolved over the past 30 plus years into a sophisticated law enforcement agency, with criminal investigators and enforcement analysts who are singularly focused on export enforcement and work closely together with licensing officers within a single bureau of the government. Using its subject matter expertise in the area of export controls, coupled with its unique administrative and other enforcement tools, Export Enforcement leverages its relationships with partner law enforcement agencies and industry to maximize its impact.

As part of the presidential Export Control Reform (ECR) initiative, BIS's jurisdiction has expanded to cover tens of thousands of munitions items transferred from the ITAR to the EAR (see below for additional information on the ECR initiative). These transfers will enhance U.S. Government oversight on such munitions exports because the specialized resources and authorities of Export Enforcement will augment the existing enforcement resources of other federal agencies dedicated to protecting U.S. national security. ECR has also created interagency information sharing and coordination mechanisms to leverage U.S. Government export enforcement and compliance resources more effectively.

Export Enforcement has three program offices: the Office of Export Enforcement (OEE), the Office of Enforcement Analysis (OEA), and the Office of Antiboycott Compliance (OAC). Export Enforcement blends the unique talents of its program offices to channel enforcement efforts against current and emerging threats to U.S. national security and foreign policy. Those unique talents are described in the following paragraphs.

### ***Office of Export Enforcement***

The Office of Export Enforcement (OEE) maintains Special Agents at offices across the United States, including its headquarters in Washington, DC, eight field offices located in Boston, Chicago, Dallas, Los Angeles, Miami, New York, Northern Virginia and San Jose, and resident offices in Atlanta, Houston and Portland. In addition, OEE Special Agents have been deployed to FBI field offices in Charlotte, Cincinnati, Denver, Huntsville, Minneapolis, Phoenix, Salt Lake City, San Diego, and Savannah, as well as to the Defense Criminal Investigative Service (DCIS) office in San Antonio, Texas, to provide enhanced coverage for investigating export violations.



OEE Special Agents are sworn federal law enforcement officers with authority to bear firearms, make arrests, execute search warrants, serve subpoenas, detain and seize items about to be illegally exported, and order the redelivery to the United States of items exported in violation of U.S. law. OEE is the only federal law enforcement agency exclusively dedicated to the enforcement of export control laws, and that singular focus allows for the development of the requisite subject matter expertise to be able to effectively enforce a complex regulatory regime. Some cases may require years of thorough investigation to bring to successful completion. OEE investigations are initiated on information and intelligence obtained from a variety of sources, including routine review of export documentation, overseas end-use monitoring, and industry information. OEE investigates both export violations by U.S. persons and the unauthorized reexport or transfer by foreign persons of items subject to the EAR to prohibited end uses, end users, or destinations. OEE works closely with other federal law enforcement agencies to identify and act on export violations and with industry to raise awareness

of compliance best practices and “red flag” indicators of potential illicit activities.<sup>2</sup> For example, OEE works with U.S. Customs and Border Protection to train outbound officers on EAR requirements to identify suspicious cargoes for detention.

Based on information gathered during the course of an investigation, OEE works closely with attorneys from the Department of Justice to prosecute violators criminally, as well as with the Office of Chief Counsel for Industry and Security to bring administrative charges. Export Enforcement also takes actions where appropriate to place parties on the BIS Entity List, Unverified List, and Denied Persons List. Export Enforcement is co-located in the same Department of Commerce bureau as Export Administration, allowing for close cooperation in the administration and enforcement of export controls. Export Enforcement provides advice and comments on the enforceability of new policies and regulations, and works closely with BIS Export Administration to routinely review export transactions to ensure compliance with the EAR. Such review includes:

- Confirming whether exported items were properly classified;
- Verifying required export authorizations, if applicable (i.e., the required export license was obtained prior to the shipment and the transaction complies with the license conditions, a license exception was available and properly used, or the item did not require a license for export to the end user and destination); and
- Determining whether the transaction involved any apparent violations of the EAR (e.g., related to the ten General Prohibitions, end use-based or end user-based controls or proscribed parties).<sup>3</sup>



*Douglas Hassebrock, OEE Director,  
Performing the Non-Exclusive Functions  
and Duties of the Assistant Secretary, at  
OEE's 2019 Special Agent Training.*

In fiscal year 2018, BIS investigations led to the criminal conviction of 30 individuals and businesses for export violations with penalties of \$618,500 in criminal fines, more than \$9.6 million in forfeitures, and 506 months of imprisonment. In addition, OEE and BIS's Office of Chief Counsel completed 43 administrative export matters, resulting in over \$1 billion in civil penalties.

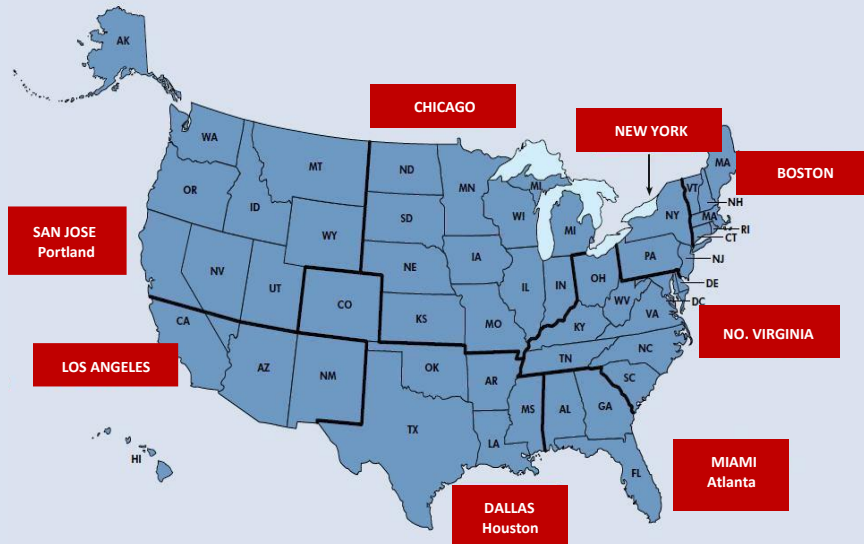
---

<sup>2</sup> An illustrative list of indicators of possible unlawful diversion is found in Supplement No. 3 to Part 732 of the Export Administration Regulations (EAR), 15 C.F.R. Parts 730 – 774.

<sup>3</sup> See Part 736 of the EAR for details on the ten General Prohibitions.

## WHERE ARE WE LOCATED

In addition to our Headquarters at the Department of Commerce in Washington, DC, Export Enforcement has eleven offices that have areas of responsibilities covering the entire United States. They are located in: Boston, Chicago, Dallas, Houston, Los Angeles, New York, Miami, Atlanta, San Jose, Portland, and Northern Virginia.



[www.bis.doc.gov](http://www.bis.doc.gov)

Export Enforcement also has Special Agents co-located with the FBI in Charlotte, Cincinnati, Denver, Huntsville, Minneapolis, Phoenix, Salt Lake City, San Diego, and Savannah, as well as with DCIS in San Antonio. Export Enforcement also has regional Export Control Officers (ECOs) in Beijing, China; Hong Kong, China; New Delhi, India; Moscow, Russia; Istanbul, Turkey; Dubai, UAE; Frankfurt, Germany; and Singapore.

## Office of Enforcement Analysis

The Office of Enforcement Analysis (OEA) supports the identification, prevention and investigation of illegal exports, reexports and transfers of items subject to the EAR and supports the prosecution of the parties responsible by: 1) analyzing the *bona fides* of foreign transaction parties to license applications (i.e., their reliability as recipients of U.S.-origin items); 2) monitoring end uses and end users of U.S.-origin exports; 3) identifying suspicious inquiries to alert U.S. companies; 4) developing investigative leads; 5) providing analytical case support; and 6) engagement with key trading partners. OEA accomplishes this mission through its Strategic Intelligence Division, International Operations Division, Export Control Officer Program, and Investigative Analysis Division.

OEA's Strategic Intelligence Division vets the *bona fides* of foreign parties to license applications and serves as the executive agent for the interagency Information Triage Unit, or "ITU." The ITU is responsible for assembling and disseminating relevant all-source information, from which to base informed decisions on proposed exports requiring a U.S. Government license.



OEA's International Operations Division screens BIS license applications and reviews export documentation to select candidates for pre-license checks (PLCs) and post-shipment verifications (PSVs), collectively referred to as end-use checks (EUCs). PLCs validate information on BIS export license applications, including end-user reliability. PSVs strengthen assurances that exporters, shippers, consignees, and end-users comply with the terms of export licenses and the EAR. This end-use monitoring program supports the export licensing process and generates information about possible export violations for further investigation by OEE. This division, working with regional Export Control Officers stationed abroad, supports Export Enforcement's role in the bilateral negotiations with, inter alia, Hong Kong, Singapore and the United Arab Emirates on export control cooperation and coordination to increase capacity to prevent the diversion of U.S.-origin items.

OEA's Export Control Officer Program consists of Special Agents on detail to the Department of Commerce's Foreign Commercial Service in seven strategic overseas locations critical to BIS's mission: Beijing, China; Hong Kong, China; Dubai, United Arab Emirates; New Delhi, India; Frankfurt, Germany; Istanbul, Turkey; and Singapore. All of these positions have regional responsibilities that extend their reach more than 50 additional countries. End-use checks are also conducted by OEE Sentinel Program trips, conducted by domestically-based OEE Special Agents and U.S. Embassy personnel. In FY2018, BIS completed 1,042 end-use checks in 50 countries.

Finally, OEA's Investigative Analysis Division is responsible for producing investigative leads relating to potential export violations for outreach and investigation by OEE Special Agents. Investigative leads are developed from unfavorable end-use checks, review of export and license data, and classified and open sources of information. In addition, OEA's Investigative Analysis Division provides research and analytical case support to OEE investigations.

### ***Office of Antiboycott Compliance***

The Office of Antiboycott Compliance (OAC) administers and enforces the antiboycott provisions of the EAR. OAC carries out its mandate through a threefold approach: monitoring boycott requests received by U.S. businesses; bringing enforcement actions when necessary; and guiding U.S. businesses on the application of the EAR to particular transactions. In addition to these traditional compliance tools, OAC liaises with foreign governments to eliminate boycott requests at their origin. By working with U.S. Government partners in the Office of the U.S. Trade Representative and at the Department of State, OAC has met with officials of boycotting countries issuing boycott-related requests. By meeting with these governments and pointing out the barrier to trade that boycott requests impose, OAC often is able to remove prohibited language, enabling U.S. businesses to compete on an equal footing in these markets.

## **Authorities and Remedies**

### ***Criminal and Civil Penalties***

In cases involving a willful violation of the EAR, violators may be subject to both criminal fines and administrative penalties. Administrative penalties may also be imposed when there is no willful intent, which means that administrative cases can be brought in a much wider variety of circumstances than criminal cases. BIS has a unique range and combination of administrative enforcement authorities including the imposition of civil penalties, denial of export privileges, and placement of individuals and

entities on lists that restrict or prohibit their involvement in export and reexport transactions. Under ECRA, criminal penalties can reach 20 years imprisonment and \$1 million per violation. Administrative monetary penalties can reach \$300,000 per violation (subject to adjustment in accordance with U.S. law, e.g., the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Pub. L. 114 -74, sec. 701) or twice the value of the transaction, whichever is greater.

The EAR provide that in appropriate cases the payment of a civil penalty may be suspended or deferred in whole or in part during a probationary period. The suspended or deferred penalty is subject to activation and collection if the probationary conditions are not fulfilled. Penalty suspensions may occur, for example, when the respondent has demonstrated, typically through the submission of financial statements and tax returns, that it is unable to pay some or all of the penalty that would be appropriate for the violations at issue. Penalties may also be suspended in whole or in part as a result of exceptional cooperation with the investigation where the agency nonetheless decides that a suspended penalty should be imposed for its deterrent effect.

BIS also may impose the requirement that the respondent hire an unaffiliated third -party consultant to conduct one or more external audits of the company's compliance with U.S. export control laws and regulations and provide a copy of the audit to Export Enforcement. A portion of the penalty amount may also be suspended for that purpose.

One of the most significant enforcement tools in the BIS arsenal is our administrative enforcement authorities. On June 22, 2016, BIS published Administrative Enforcement Guidelines that entered into force on July 22, 2016. The Guidelines, set forth in Supplement No. 1 to Part 766, capture the administrative enforcement policies and procedures of our Office of Export Enforcement, or "OEE", in several ways. First, the Guidelines outline the following four categories of Factors affecting administrative sanctions: 1) Aggravating Factors; 2) General Factors that could be considered either aggravating or mitigating depending upon the circumstances; 3) Mitigating Factors; and 4) other Relevant Factors on a case- by-case basis, such as related violations or other enforcement action.

Additionally, the Guidelines formally account for the substantial increase in the maximum penalties for violations of the EAR and distinguish between egregious and non-egregious civil monetary penalty cases. Finally, reference in the Guidelines to "transaction value" provides sufficient flexibility to allow for the determination of an appropriate transaction value in a wide variety of circumstances. Amounts set forth in a schedule provide for a graduated series of penalties based on the underlying transaction values, reflecting appropriate starting points for penalty calculations in non-egregious cases not voluntarily disclosed to OEE. The base penalty amount for a non-egregious case involving a VSD equals one-half of the transaction value, capped at the statutory maximum per violation of the EAR. The base penalty amount for cases deemed to be egregious brought to OEE's attention by means other than a VSD shall be an amount up to the statutory maximum. For those egregious cases involving a VSD, the base penalty amount shall be an amount up to half the statutory maximum.

## INCREASING TRANSPARENCY THROUGH PENALTY GUIDANCE

BIS provides guidance (found in Supplement No. 1 to Part 766 of the EAR) to provide the public with a comprehensive description of how BIS determines appropriate penalties in the settlement of administrative export control enforcement cases. It explains that BIS carefully considers each settlement in light of the facts and circumstances of the case, relevant precedent, and BIS's objective to achieve an appropriate level of penalty and deterrent effect.

The penalty guidance can be found online at

<https://www.bis.doc.gov/index.php/documents/pdfs/1567-administrative-enforcement-guidelines/file>

Several factors are taken into account when determining the appropriate administrative penalty. The penalty guidance encourages parties to provide information to BIS that would be helpful in the application of the guidance to their cases. Some factors are given up to a specific percentage of mitigation and are treated as considerably more significant than factors that are not so designated. The Factors set forth in the Guidelines are reconstituted into the following:

### **Aggravating Factors**

- A. Willful or Reckless Violation of Law
- B. Awareness of Conduct at Issue
- C. Harm to Regulatory Program Objectives

### **General Factors**

- D. Individual Characteristics
- E. Compliance Program

### **Mitigating Factors**

- F. Remedial Response
- G. Exceptional Cooperation with OEE
- H. License Was Likely To Be Approved

### **Other Relevant Factors Considered on a Case-by-Case Basis**

- I. Related Violations
- J. Multiple Unrelated Violations
- K. Other Enforcement Action
- L. Future Compliance/Deterrence Effect
- M. Other Factors that OEE Deems Relevant

## ***Voluntary Self-Disclosures***

Export Enforcement at BIS encourages the submission of voluntary self-disclosures (VSDs) by parties who believe they may have violated the EAR. VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements. Parties can submit an initial disclosure when the violations are first uncovered and follow-up with a complete narrative within 180 days.<sup>4</sup> OEE carefully reviews VSDs received from disclosing parties to determine if violations of the EAR have occurred and to determine the appropriate corrective action when violations have taken place. Most VSDs are resolved with the issuance of a warning letter. Should OEE determine that the issuance of an administrative penalty is appropriate for the resolution of a VSD, 50 percent mitigation is accorded the VSD in assessing the penalty. In appropriate cases, fines and other administrative penalties may be significantly reduced and/or suspended for a probationary period. During

---

<sup>4</sup> See Section 764.5 of the EAR for details on how to submit a VSD.

fiscal year 2018, OEE opened approximately 409 VSD cases and closed approximately 409 VSD cases. Around 81% of these VSD cases were closed with the issuance of a warning letter, while around 14% were closed with “no action” or “no violation.”

Of the 409 VSDs submitted during fiscal year 2018, approximately one-third involved the CCL’s 600 series commodities. Less than 1% of all VSD cases were closed with the issuance of administrative sanctions during fiscal year 2018. Generally speaking, the vast majority of all of our investigations involving 600 series or License Exception Strategic Trade Authorization (STA) violations have been the result of VSDs.

VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements in the present and the future. Warning letters will generally be issued in cases involving inadvertent violations and cases involving minor or isolated compliance deficiencies, absent the presence of aggravating factors.

### ***Denial of Export Privileges***

BIS has the authority and discretion to deny all export privileges under the EAR of a domestic or foreign individual or company. Consider the potentially catastrophic impact upon a person or organization of not being able to export, reexport, or receive any item – including an EAR99 item – that is subject to the EAR. BIS may impose a denial of export privileges as a sanction in an administrative case, or as a result of a person’s criminal conviction under certain statutes. A denial of export privileges prohibits a person from participating in any transactions subject to the EAR. Furthermore, it is unlawful for other businesses and individuals to participate in an export transaction subject to the EAR with a denied person.

Denial of export privileges may be imposed as part of an administrative penalty. Under Section 1760(e) of ECRA, a denial of export privileges may be imposed for up to ten years from the date of a person’s conviction under the EAR, IEEPA, or Section 38 of the Arms Export Control Act (or any regulation, license, or order issued thereunder), or one of the several espionage, conspiracy and smuggling-related statutes. In cases where no administrative charges are brought, there is no limit to the period of export denial. The standard terms of a BIS denial order are published in Supplement No. 1 to Part 764 of the EAR. (Note: 1760(e) section does not apply to convictions of antiboycott violations)

In addition, the Assistant Secretary for Export Enforcement may issue a Temporary Denial Order (TDO) denying any, or (typically) all, of the export privileges of a company or individual to prevent an imminent or ongoing export control violation. These orders are issued ex parte for a renewable 180 -day period and deny not only the right to export from the United States, but also the right to receive or participate in exports from the United States. TDOs are also described in Section 766.24 of the EAR.

### ***BIS-Administered Lists***

The Department of Commerce maintains three screening lists which advise the exporting public that listed persons are subject to specific restrictions. In the event an entity, company, or individual on one of the following lists appears to match a potential party in an export transaction, additional due diligence is required before proceeding to ensure the transaction does not violate the EAR. These lists are available on the BIS website at <http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern>. They are also included in the U.S. Government Consolidated Screening List, a comprehensive screening system managed by the Departments of State, Treasury and Commerce, available at <https://www.export.gov/article?id=Consolidated-Screening-List>



## Denied Persons List

The Denied Persons List contains the names and addresses of individuals and entities located in the United States and overseas subject to a denial of export privileges. Any dealings with a person or entity on this list that would violate the terms of the denial order are prohibited. See Section 764.3(a)(2) of the EAR.

## Entity List

The BIS Entity List has evolved into a formidable administrative enforcement tool that prohibits unlicensed exports, reexports, or transfers of some or all items subject to the EAR to listed foreign entities. Those on the Entity List were placed there because of the risk they pose of diversion of U.S.-origin items to weapons of mass destruction (WMD) programs, destabilizing accumulations of conventional weapons, terrorism, or other activities contrary to U.S. national security or foreign policy interests. These license requirements are in addition to any license requirements imposed on the transaction by other provisions of the EAR. As a general rule, BIS applies a policy of denial for license applications involving listed entities. General Orders also may restrict exports to named individuals or entities. For General Orders, see Supplement No. 1 of Part 736 of the EAR. The Entity List also serves as an incentive for listed foreign parties to implement effective internal compliance programs to stop the diversion of U.S.-origin items to unauthorized destinations, uses, or users, thereby providing a basis for removal.

For guidance concerning the prohibitions and license application review policy applicable to a particular entity, please review that individual or organization's entry on the list. Listed entities may request removal from the Entity List by submitting a petition pursuant to Section 744.16 and Supplement 5 to Part 744 of the EAR.

## Unverified List

The Unverified List (UVL) contains the names and addresses of foreign persons that have been parties or intended parties to transactions subject to the EAR whose *bona fides* could not be confirmed as a result of an end-use check, including the U.S. Government's inability to conduct such an end-use check. The presence of a person listed on the Unverified List in a proposed export transaction creates three consequences: all export transactions must be reported in the Automated Export System (AES) (see Section 758.1(b)(8) of the EAR); license exception-eligibility is suspended (see Section 740.2(a)(17) of the EAR); and for all other EAR transactions not subject to a license requirement, the exporter must obtain a statement from the UVL party agreeing to abide by the EAR, including to permit an end-use check prior to export (see Section 744.15 of the EAR). Once BIS confirms the *bona fides* of the foreign party, including through completion of an end-use check, a party may be removed from the UVL. Similar to the Entity List, the UVL provides an incentive for foreign companies to comply with the EAR, including its end-use check requirements.

## Asset Forfeiture

Asset forfeitures target the financial motivation underlying many illicit export activities. The forfeiture of assets obtained in the conduct of unlawful activity may be imposed in connection with a criminal conviction for export violations or in a civil forfeiture action. Asset forfeitures prevent export violators from benefiting from the fruits of their crimes and the value of forfeited assets can greatly exceed criminal fines or administrative penalties.

## ***False Statements***

A party to an export transaction may be subject to criminal and/or administrative sanctions for making false statements to the U.S. Government in connection with an activity subject to the EAR. Most frequently, the false statements are made on an export document or to a federal law enforcement officer. Common types of false statements seen by OEE are: 1) statements on Electronic Export Information or EEI (information now filed through the Automated Export System (AES), but formerly filed as a paper Shipper's Export Declarations (SED)) that an export is destined for one country when it is really destined for a sanctioned destination; 2) SED or AES filing statements that the export does not require a license (i.e., it is "NLR") when in fact a license is required for the shipment; 3) false item valuations; and 4) statements that an export was shipped under a particular license number when in fact that license was for a different item. False statements that are made to the U.S. Government indirectly through another person, such as a freight forwarder, may constitute violations of the EAR.



*OEE Special Agents conducting an inspection.*

## **Export Compliance**

### ***Responsible Parties***

All parties that participate in transactions subject to the EAR must comply with the EAR. These persons may include exporters, freight forwarders, carriers, consignees, and other participants in an export transaction. The EAR apply not only to parties in the United States, but also to persons in foreign countries who are involved in transactions subject to the EAR.

### ***Due Diligence: Eight Principles for an Effective Compliance Program***

Many exports of controlled items, including software and technology, require a license from BIS. It is the responsibility of the exporter to obtain a license when one is required under the EAR. License requirements for a particular transaction, as described in the EAR, are based on a number of factors, including technical characteristics of the item to be exported and the item's destination, end user, and end use. When determining whether a license is required for your transaction, you should be able to answer the following questions:

- ☐ **What is being exported?**
- ☐ **Where is the item being exported?**
- ☐ **Who will receive the item?**
- ☐ **How will the item be used?**

#### **PREVENTIVE MEASURES YOU CAN TAKE**

- Check exporters and customers
- Check end users and end uses
- Review Automated Export Declarations
- Educate relevant personnel

BIS weighs a variety of aggravating and mitigating factors in deciding the level of penalties to assess in administrative cases. As set forth in Supplement Nos. 1 and 2 to Part 766 of the EAR, an effective compliance program may be entitled to significant mitigation. BIS's Export Management Compliance Program (EMCP) guidelines can be accessed through BIS's website at [www.bis.doc.gov](http://www.bis.doc.gov) under the Compliance and Training tab.

BIS employs the following eight guiding principles when assessing the effectiveness of a company's export compliance program:

- 1. Have strong and continuous Management Commitment. In order to build and maintain an effective program senior management must:
  - Publicly support compliance policies and procedures
  - Provide sufficient resources
  - Support export compliance training and training sessions
- 2. Identify and mitigate your organization's potential vulnerabilities by conducting frequent Risk Assessments.
- 3. Write and implement Export Authorization procedures on jurisdiction, classification, licensing and screening. This is vital for preventing your organization from exporting unauthorized items and possibly facing export penalties.
- 4. Assign individuals roles in Recordkeeping and ensure procedures meet the requirements in EAR § 762.4.
- 5. Require Training for all employees, including support staff, whose responsibilities relate to exports in order to keep up with changing regulations and to network with other export compliance practitioners.
- 6. Perform regular Audits to gauge how well procedures are implemented and how elements need to be augmented.
- 7. Implement a program to Handle Compliance Issues, including how to prevent export violations and how to complete corrective actions when a violation is found.
- 8. Whether writing an ECP for the first time or maintaining an ECP, make sure to keep the manual current and relevant to the members of your organization.

Developing an effective company compliance program is essential not only for preventing export violations, but also for enabling BIS to differentiate violations by individual employees from larger patterns of corporate noncompliance. Export Enforcement may afford significant mitigation to companies with effective compliance programs and will emphasize individual responsibility when seeking penalties against willful violations by employees.

If you need assistance to determine whether the item you want to export requires a license you should:

1. Check the BIS website <http://www.bis.doc.gov>, or
2. Call one of our export counselors at 202-482-4811 (Washington, DC) or 949-660-0144 (California) for counseling assistance.

Please note that, whether you are the exporter, freight forwarder, consignee, or other party to the transaction, you must address any red flags that arise. Taking part in an export transaction where a license is required but not obtained may subject you to criminal and/or administrative liability. The EAR discusses red flags in Supplement No. 3 to Part 732, which is available on the BIS website.

A key in determining whether an export license is required from the Department of Commerce involves knowing whether the item for export has a specific ECCN, an alpha-numeric code that describes a particular item or type of item, and shows the controls placed on that item. All ECCNs are listed on the CCL. Once an item has been classified, the next step is to determine whether an export license is required based on the “reasons for control” of the item and the country of ultimate destination. Reasons for control include chemical and biological weapons controls, nuclear nonproliferation, national security, missile technology, regional stability, and crime control. Please visit <https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification> for more information on how to classify items.

### ***Transshipments & Reexports***

Parties to an export transaction cannot bypass the EAR by shipping items through a third country. The transshipment or reexport of items in international commerce may be a violation of U.S. law. For example, an exporter cannot bypass the U.S. embargo against Iran by shipping an item to a distributor in the United Kingdom and asking that distributor to transship the item to a customer in Iran. Under U.S. law, this would be considered an export to Iran, even though it does not go directly to that country, and both the U.S. exporter and the United Kingdom distributor could be liable for violating U.S. law.

Parties to exports or reexports of items subject to the EAR should be alert to the red flag indicators of possible unlawful diversion found in Supplement No. 3 to Part 732 of the EAR, and should consult BIS’s guidance on reexports at: <http://www.bis.doc.gov/index.php/licensing/reexports-and-offshore-transactions>.

In addition, exporters should be knowledgeable about the export control requirements of their customers and are strongly encouraged to obtain copies of any relevant import licenses (permits) prior to export. For example, Hong Kong requires all importers to receive a license prior to receipt of multilaterally -controlled items from abroad. The EAR requires exporters or reexporters to Hong Kong of any item subject to the EAR and controlled on the CCL for NS, MT, NP Column 1, or CB reasons to obtain a copy of the Hong Kong import license or a written statement that no such license is necessary. (See Section 740.2(a)(19), (20) of the EAR). Similarly, exporters are required to notify their customers of export license conditions (e.g., requirement for BIS authorization for subsequent transfer (in-country) or reexport) and should make their customers aware that a license (permit) may be required for subsequent reexport from their own government in addition to BIS. BIS published guidance on its website to assist exporters in this regard: <https://www.bis.doc.gov/index.php/licensing/9-bis/carousel/689-foreign-import-export-license-requirements-hong-kong-singapore-united-arab-emirates>

### ***Catch-All Controls***

BIS controls exports of items not only based on their technical specifications, but also based on their intended end use and end user. The EAR imposes license requirements on exports of items subject to the EAR if the exporter knows or has reason to know that any of the items will be used in an end-use of particular concern to the U.S. Government, such as a missile or nuclear weapons program, or in certain circumstances a military end use or by a military end user. These controls are often referred to as “catch-all” controls because they apply to a broad set of items, or in the case of WMD activities, to any item subject to the EAR, even if the item would not ordinarily require a license based on its technical specification.



Export restrictions based on the end use and end user are specified in Part 744 of the EAR and include restrictions on certain nuclear, rocket system, chemical and biological, and military end uses, as well as restrictions on certain end users. BIS maintains restrictions on end users listed on the Denied Persons List, the Entity List, and the Unverified List. BIS uses these lists to notify the public of end users of concern, including entities engaged in illicit export activity or other activities contrary to U.S. national security or foreign policy, and entities that could not be confirmed as reliable recipients of U.S.-origin commodities, software, or technology.

The EAR also incorporate by reference certain entities sanctioned by the Department of the Treasury, including certain Specially Designated Nationals, Specially Designated Global Terrorists, and Foreign Terrorist Organizations.

These lists are not comprehensive and do not relieve parties to an export transaction of their responsibility to determine the nature and activities of potential customers who may not be listed (see BIS's "Know Your Customer" Guidance in Supplement No. 3 to Part 732 of the EAR, available on the BIS website).

### ***Successor Liability***

Businesses can be held liable for violations of the EAR committed by companies that they acquire. Businesses should be aware that the principles of successor liability may apply to them and should perform "due diligence" in scrutinizing the export control practices of any companies that they plan to acquire. A properly structured due diligence review can determine whether an acquired company has violated any export laws. This review should examine the company's export history and compliance practices, including commodity classifications, technology exchanges, export licenses and authorizations, end users, end uses, international contracts, the status of certain foreign employees who have access to controlled technologies, and the company's export policies, procedures, and compliance manuals. Voluntary self-disclosures should be submitted outlining any violations that this review uncovers, if not by the company responsible, then by the company seeking to acquire it. Failure to scrutinize properly an acquired company's export practices can lead to liability being imposed on the acquiring company.

### ***Educational Outreach***

To raise awareness of export control requirements and prevent potential violations of the EAR, Export Enforcement conducts educational outreach to U.S. exporters and foreign trade groups. In addition to participating in BIS export control seminars and conferences, Export Enforcement conducts outreach to individual exporters to inform them of their responsibilities under the EAR, review compliance best practices, and alert them if appropriate to offshore illicit procurement activities that they may be a target of. Export Enforcement also engages American business communities overseas and foreign trade and industry associations to promote awareness of U.S. export and reexport controls, including in cooperation with foreign government partners.

During FY2018, OEE conducted over 1,600 outreaches. Industry's knowledge and compliance with the EAR establishes a built-in warning system for Export Enforcement to be aware of suspicious actors. Coupled with this general outreach, Export Enforcement has expanded its Guardian outreach program to industry, alerting companies of suspicious parties that may be seeking to obtain sensitive items. OEE fully appreciates the reputational risk associated with your items being involved in illicit activities, and this advance warning System is meant to help you identify otherwise unforeseen risks in potential transactions.

## ***Cyber-Intrusions and Data Exfiltration***

One of the new areas of focus in our outreach efforts relates to cyber-intrusions and data exfiltration that result in your controlled technology being exported. It is becoming almost a daily occurrence to read about a cyber-intrusion or attack. The perpetrators of cyber-crime are varied; they include independent hackers and criminal organizations, as well as state actors. The theft of export controlled information from your



computer systems as a result of foreign cyber actors is a threat to U.S. national security interests and your company's competitive lifeblood: intellectual property.

The U.S. Government is attempting to address this looming menace through a whole-of-government approach. On February 12, 2014, the National Institute of Standards and Technology, a sister agency at the Department

of Commerce, published the first National Cybersecurity Framework, which can be found at [www.nist.gov/cyberframework](http://www.nist.gov/cyberframework). An updated version was released in April 2018. Regardless of the type of business sector or an organization's size, an entity can use the framework to determine its current level of cybersecurity, set goals for cybersecurity that are in sync with its business environment, and establish a plan for improving or maintaining its cybersecurity. This Framework also offers a methodology to protect privacy and civil liberties to help organizations incorporate those protections into a comprehensive cybersecurity program. The Framework is part of a larger initiative to combat the ever evolving cyber threat. Both the FBI and the Department of Homeland Security's Office of Infrastructure Protection are developing programs and initiatives to help the private sector protect, identify, mitigate and report malicious cyber activity and actors.

Evaluate whether you need to incorporate cybersecurity into your company's export compliance program as well as report cyber incidents. Reporting the exfiltration of controlled technology is separate and distinct from submitting a voluntary self-disclosure (VSD). The latter involves your discovery of a violation of the EAR committed by your company. By reporting cyber thefts, you are giving us critical information that can allow BIS, working with our interagency partners, to identify these cyber-actors and bring our unique BIS tools to bear against them. Cybersecurity, like effective export controls, can only be achieved with your support and partnership.

# Chapter 1 – Terrorism and State Sponsors of Terrorism

## Introduction

The United States maintains broad export controls on certain countries for foreign policy reasons. It has imposed such controls unilaterally or multilaterally pursuant to United Nations Security Council Resolutions. Countries may be subject to partial or comprehensive embargoes, in some cases as a consequence of their designation by the Secretary of State as state sponsors of terrorism. As of the date of publication of this document, Syria, Iran, and Sudan remain designated as state sponsors of terrorism. BIS implements stringent export controls on these three countries under the EAR as well as on Cuba and North Korea.<sup>5</sup> As a practical matter, many exports of ordinary commercial items not typically controlled to other destinations may require authorization from BIS and other federal agencies, including the Department of the Treasury's Office of Foreign Assets Control (OFAC). For these five countries, BIS or OFAC – and in some cases both agencies together – administer the licensing requirements and enforce the controls.



### What is OFAC and what does it do?

The Office of Foreign Assets Control (OFAC) administers and enforces economic sanctions programs against countries, entities, and individuals, including terrorists and narcotics traffickers. The sanctions may be either partial or comprehensive, requiring the blocking of assets of designated persons in some situations or the imposition of broad trade restrictions on regions and sectors to accomplish foreign policy and national security goals.

BIS and OFAC work together to administer and enforce the sanctions against Iran and both maintain license requirements for Iran. To reduce duplication with respect to these licensing requirements, exporters or reexporters are not required to seek separate authorization from BIS for an export or reexport subject both to the EAR and to the Iranian Transactions and Sanctions Regulations (ITSR). If OFAC authorizes an export or reexport, such authorization is considered authorization for purposes of the EAR as well. It is important to note that transactions that are not subject to OFAC regulatory authority may require BIS authorization. No person may export or reexport any item that is subject to the EAR if such transaction is prohibited by the ITSR and not authorized by OFAC. This prohibition applies whether or not the EAR independently require a license for export or reexport. Please see section 746.7 of the EAR or visit <http://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/iran> for more information.

<sup>5</sup> On October 11, 2008, the United States rescinded the designation of North Korea as a State Sponsor of Terrorism pursuant to Section 6(j) of the Export Administration Act of 1979 and several other statutes. However, North Korea remains in Country Group E:1 (terrorist supporting countries) under the EAR along with Iran, Sudan, and Syria and thus remains subject to all applicable EAR prohibitions. On May 29, 2015, the United States rescinded the designation for Cuba. However, Cuba remains subject to a comprehensive embargo, and the export and reexport of all items subject to the EAR still require authorization from BIS.

It is important to familiarize yourself with the restrictions that apply to the ultimate destination of your export. U.S. law in this area frequently changes in accordance with an evolving foreign policy. The following websites are good resources:

**OFAC's website:**

<http://www.treasury.gov/ofac>

**BIS's website:**

<http://www.bis.doc.gov>

## Criminal and Administrative Case Examples

### David Levick / ICM Components

---

**The Violation:** On February 1, 2019, Australian national David Levick pled guilty to charges related to his involvement in the procurement and shipment of U.S.-origin items, including aircraft parts classified under ECCN 9A991 and controlled under the U.S. Munitions List, to Iran. Levick, the General Manager of ICM Components, Inc. in Thornleigh Australia, solicited purchase orders and business for aircraft parts from a representative of a trading company in Iran. This individual in Iran also operated and controlled companies in Malaysia that acted as intermediaries for the Iranian trading company. Levick then placed orders with U.S. companies on behalf of the Iranian individual for the goods, which included aircraft parts, precision pressure transducers that have a wide variety of applications in the avionics industry, emergency flotation systems kits designed for use on Bell 206 helicopters to assist when landing in water or soft desert terrain, and shock mounted light assemblies designated for high vibration use that can be used on helicopters and other fixed wing aircraft. When necessary, Levick used a broker in Tarpon Springs, Florida, through whom orders could be placed for the parts to further conceal that they were intended for transshipment to Iran. Levick intentionally concealed the ultimate end use and end users of the parts from manufacturers, distributors, shippers, and freight forwarders located in the United States and elsewhere. In addition, Levick and others structured their payments between each other for the parts to avoid trade restrictions imposed on Iranian financial institutions by other countries. Levick and ICM Components wired money to companies in the United States as payment for the parts. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the Federal Bureau of Investigation (FBI), Immigration and Customs Enforcement (ICE), and Defense Criminal Investigative Service (DCIS).

**The Penalty:** On March 21, 2019, Levick was sentenced in U.S. District Court for the District of Columbia to 24 months in prison, 12 months of supervised release, a \$199,227 forfeiture, a \$400 special assessment, and deportation upon completion of his sentence.

### Arash Sepehri / Tajhiz Sanat Shayan

---

**The Violation:** Between 2008 and 2014, Iranian citizen Arash Sepehri, an employee and on the board of directors of Tehran-based Tajhiz Sanat Shayan (TSS), conspired with individuals and companies operating in Hong Kong, the United Arab Emirates (UAE), and Iran to send hundreds of thousands of dollars' worth of U.S.-origin goods and technology, most with military applications, to Iran. TSS and other companies involved in the conspiracy were listed by the European Union on May 23, 2011, as entities being sanctioned for their involvement in the procurement of components for the Iranian nuclear program. Sepehri and his conspirators relied on well-known techniques to evade export controls and sanctions including the use of aliases, front companies, and circuitous shipping and payment methods. These techniques allowed Sepehri to conceal both the true end users and intended use of the procured goods. Through TSS and associated companies, Sepehri and others conspired to obtain high-resolution sonar equipment, data input boards, laptops, and acoustic transducers classified under ECCN 6A991 and designated EAR99, as well as a lens for a missile tracking device controlled under the International Traffic in Arms Regulations (ITAR), to Iran via Hong Kong and the UAE. In June 2018, Sepehri was returned to the United States based on an Interpol Diffusion Notice. On November 7, 2018, Arash Sepehri, pled guilty in U.S. District Court for the District of Columbia for his role in the scheme. This case resulted from a joint investigation conducted by OEE's Washington Field Office, ICE and the FBI.



**The Penalty:** On February 26, 2019, Arash Sepehri was sentenced to 25 months in prison with credit for time served, a \$100 special assessment and a \$125,661 forfeiture.

## **Arzu Sagsoz / Kral Havacilik**

---

**The Violation:** On October 4, 2018, Arzu Sagsoz pled guilty in the U.S. District Court for the District of Columbia to conspiracy to violate IEEPA. Sagsoz was arrested on September 27, 2017 by law enforcement authorities at the Batumi International Airport in the country of Georgia pursuant to an Interpol Red Notice submitted by BIS. After a period of detention in Georgia, Sagsoz was extradited to the United States and was arrested and processed upon her arrival at Washington Dulles International Airport. Sagsoz operated as a corporate employee of Turkish Aviation Supply Company, Kral Havacilik, which was responsible for illegally supplying the Iranian airline Mahan Air with U.S.-origin aircraft parts. Mahan Air has been subject to a BIS Temporary Denial Order since 2008. In 2011, Mahan Air was also added to the Office of Foreign Assets Control Special Designated National's list for Mahan Air's support of global terrorism. This case resulted from an investigation conducted by OEE's Atlanta Resident Office and Washington Field Office.

**The Penalty:** On January 10, 2019, Arzu Sagsoz was sentenced to 20 months in prison, with credit for time served in the country of Georgia, one year of probation, and a \$100 special assessment.

## **Ali Caby / Marjan Caby / Arash Caby**

---

**The Violation:** In February 2017, Iranian nationals Ali Caby, Marjan Caby, and Arash Caby were arrested in connection with a conspiracy to illegally export aviation parts classified under ECCN 9A991 to Syrian Arab Airlines, which appears on the Office of Foreign Assets Control's Specially Designated Nationals List for transporting weapons and ammunition to Syria in conjunction with terrorist organization Hizballah, and the Iranian Revolutionary Guard Corps. Ali Caby ran the Bulgaria office of AW-Tronics, a Miami, Florida-based export company that was managed by Arash Caby, and which shipped and exported various aircraft parts and equipment to Syrian Arab Airlines. Ali Caby and Arash Caby closely supervised and encouraged subordinate employees of AW-Tronics in the willful exportation of the parts and equipment to SDN Syrian Air, whose activities have assisted the Syrian government's violent crackdown on its people. Marjan Caby, as AW-Tronics' export compliance officer and auditor, facilitated these exports by submitting false and misleading electronic export information to federal agencies. This case resulted from a joint investigation conducted by OEE's Miami Field Office, the FBI, ICE, and DCIS.

**The Penalty:** On December 19, 2017, Ali Caby, Marjan Caby, and Arash Caby were sentenced in U.S. District Court for the Southern District of Miami. Ali Caby was sentenced to two years in prison, two years of supervised release and a \$100 special assessment. Marjan Caby was sentenced to one year and one day in prison, two years of supervised release and a \$100 special assessment. Arash Caby was sentenced to two years in prison, two years of supervised release, a \$10,000 criminal fine and a \$100 special assessment. All three defendants were also subject to a shared \$35,000 forfeiture as part of the plea agreement.

## **Ali Eslamian**

---

**The Violation:** Between 2011 and 2012, Ali Eslamian took actions prohibited by a BIS Temporary Denial Order (TDO) issued against him in August 2011. Eslamian was added to an existing BIS TDO, the primary respondent of which was Mahan Air, an Iranian airline. Eslamian violated the TDO issued against him by participating in a transaction subject to the EAR by carrying on negotiations and ordering an aircraft engine subject to the EAR. Specifically, Eslamian ordered an aircraft engine classified under ECCN 9A991 and controlled for anti-terrorism reason from a Brazilian airline. Despite the TDO's broad prohibitions against Eslamian participating in any way in any transactions subject to the EAR, he continued his efforts to acquire the aircraft engine even after the Brazilian airline raised concerns about his "name appearing on a U.S. Government sanctions list as affiliated with Iranian airline." Eslamian responded by misleadingly stating that he only "recently" had been added to the TDO and that he was not subject to U.S. Government sanctions, asserting that the TDO applied "to the U.S. exports by U.S. companies only." This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On September 28, 2017, Ali Eslamian agreed to pay a \$250,000 civil penalty, \$150,000 of which was suspended provided no violations occur during a four-year probationary period. In addition, a four-year denial of export privileges was imposed on Eslamian which was suspended provided that during the suspension period Eslamian commits no future violations and pays the civil penalty. Eslamian's companies, Skyco (UK) Ltd. and Equipco (UK), were each listed as a Related Party on the Final Order, and both were also subject to the four-year suspended denial of export privileges.

## **Worthington Products, Inc. / Hydel Engineering Products**

---

**The Violation:** From 2009 through 2012, Narender Sharma and Hydel Engineering Products (Hydel), located in India, conspired with Paul Meeks and Worthington Products, Inc. (WPI) of Canton, Ohio to evade the U.S. embargo against Iran. Sharma and Meeks schemed to sell and export U.S.-origin waterway barrier debris systems designated EAR99 and related components to Iran via transshipment through the United Arab Emirates, including to Mahab Ghodss, an Iranian Government entity, without the required U.S. Government authorization. The conspirators specifically discussed omitting any reference to Iran in the transaction documentation relating to the shipment of the waterway barrier debris system, and considered various transshipment routing schemes at length before ultimately deciding to transship the item through the United Arab Emirates. Sharma traveled to Iran in 2010 to meet with Mahab Ghodss and to pursue other Iranian customers, including other entities part of, or funded by, the Iranian Government. Before and after this trip to Iran, Meeks responded to inquiries from entities in Iran by forwarding them to Sharma and telling the Iranians that Hydel was WPI's agent for Iran and the surrounding region. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On August 31, 2017, Narender Sharma and Hydel Engineering Products agreed to pay a civil penalty of \$100,000, \$70,000 of which was suspended provided that no further violations occur during a five-year probationary period. Additionally, Sharma and Hydel's export privileges were denied for a period of five years (suspended during the five-year probationary period and thereafter waived, provided no violations are committed during the probationary period). On June 17, 2016, Paul Meeks and Worthington Products, Inc. agreed to pay a civil penalty of \$250,000 and were ordered to complete export controls compliance training annually for five years. Additionally, Meeks and WPI's export privileges were denied for a period of five years (suspended during the five-year probationary period and thereafter waived, provided no violations are committed during the probationary period).

## **Hassan Zafari**

---

**The Violation:** In September 2014, Hassan Zafari, aka Sam Zafari, caused, aided or abetted the export from the United States to Iran, via the United Arab Emirates (UAE), of a used industrial laser system subject to the EAR and valued at approximately \$12,000, without the required U.S. Government authorization. The laser system, designated EAR99, is also subject to the Iranian Transactions Regulations. Zafari was aware that U.S. law prohibited exports to Iran and that items could not ship through third countries to a final destination that was an embargoed destination, as he admitted to BIS Special Agents during an interview. Nonetheless, Zafari took several actions that facilitated the transaction, including identifying and hiring a freight forwarding company to ship the laser system to the UAE, and instructing the forwarder to list the UAE general trading company as the consignee while aware that the item actually was intended for transshipment to Iran. Zafari also suggested to the Iranian purchaser that he create a revised bill of lading after delivery in the UAE, to facilitate the transshipment through the UAE to Iran. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On June 28, 2017, Hassan Zafari agreed to pay a \$52,500 civil penalty, \$45,000 of which was suspended provided no violations occur during a two-year probationary period.

## Erdal Akova / Esa Kimya

---

**The Violation:** On March 8, 2017, Turkish national Erdal Akova pled guilty in U.S. District Court for the Northern District of Georgia in connection with a conspiracy to export military grade epoxy to Iran for final use by the Iran Aircraft Manufacturing Industrial Company (HESA). The U.S. Department of the Treasury designated HESA as an entity with roles in Iran's nuclear and ballistic missile programs and because it has provided support to the Iranian Revolutionary Guard Corps. Akova knowingly allowed his name and his company's name to be used to purchase epoxy destined for Iran. He also allowed his company in Turkey, Esa Kimya, to be used as the transshipment location for the epoxy ultimately destined for delivery to Iran. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, ICE, and the FBI.

**The Penalty:** On March 8, 2017, Akova was sentenced to 36 months in prison and a \$200 special assessment.

## Mansour Zadeh

---

**The Violation:** On October 27, 2016, Mansour Zadeh pled guilty in U.S. District Court for the District of Columbia in connection with the reexport of U.S.-manufactured aircraft products classified under ECCN 9A991 to Iran through Cyprus. Zadeh, an Iranian national, was arrested in Colorado in June 2016 related to violation of a BIS Temporary Denial Order and smuggling. This case resulted from a joint investigation conducted by OEE's Boston Field Office, ICE and the FBI.

**The Penalty:** On December 14, 2016, Zadeh was sentenced to eight months in prison, one year of probation, a \$69,159 forfeiture, and a \$100 special assessment.

## National Oilwell Varco / Dreco Energy Services Ltd.

---

**The Violation:** On 21 occasions between 2006 and 2007, Dreco Energy Services Ltd. of Canada caused, aided and/or abetted the export from the United States to Iran, via Canada, of EAR99 U.S.-origin oil and gas equipment valued at \$2,315,253 without the required authorization. After ordering and obtaining the items from the United States without disclosing that the items were intended to fulfill orders from Iranian customers, Dreco Energy Services Ltd. transshipped the items from Canada to Iran, and specifically to the National Iranian Drilling Company and to Kala Naft, the procurement arm of the National Iranian Oil Company. In 2012, National Oilwell Varco (NOV) sold and/or transferred filament winder mandrels valued at \$69,615 to Oman. The filament winder mandrels were classified under ECCN 1B201 and required a BIS export license. NOV had applied for and received an export license from BIS for a total of nine filament winder mandrels, but instead exported a total of 21 of the items. This case resulted from a joint investigation conducted by OEE's Houston Resident Office and ICE.

**The Penalty:** On November 8, 2016 NOV signed a Non-Prosecution Agreement (NPA) with BIS, DOT, OFAC, ICE, and DOJ. The NPA specifies that NOV forfeit \$22,500,000 in funds to the DOT Forfeiture Fund. Additionally, on November 8, 2015, Dreco Energy Services Ltd. and NOV agreed to pay a \$2,500,000 civil penalty to BIS.

## Tayabi Fazal Hussain / Prime P.E. International Trading Company

---

**The Violation:** On June 30, 2016, Indian national Tayabi Fazal Hussain pled guilty in connection with the export of numerous U.S.-origin goods, including optical and telescopic equipment and several sets of mobile gas turbine generators, valued at \$8,700,000 per unit, for transshipment from the United Arab Emirates to Iran. Hussain, Finance Manager for Prime P.E. International Trading Company located in the United Arab Emirates, was arrested when he arrived in the United States in November 2015. Hussain pled guilty to the charges on June 30, 2016. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, the FBI and ICE.

**The Penalty:** On October 3, 2016, Tayabi Fazal Hussain was sentenced U.S. District Court for the Northern District of Indiana to 15 months in prison and a \$100 special assessment. In addition, on September 28, 2017, a nine-year denial order was imposed against Hussain.

## Harold Rinko / Ahmad Feras Deri / Global Parts Supply

---

**The Violation:** On May 26, 2016, Ahmad Feras Deri pled guilty to conspiracy to violate the IEEPA. On September 16, 2014, Rinko, owner-operator of Global Parts Supply in Hallstead, Pennsylvania, pled guilty in connection with the unlicensed export of items from the United States to Syria through Jordan, the United Arab Emirates, and the United Kingdom. Rinko, Deri and one other defendant were indicted in 2012 for preparing false invoices which undervalued and mislabeled the goods purchased and listed false identities and locations of the purchasers. Deri was extradited in November 2015 from the United Kingdom. The items involved included a portable gas scanner; handheld instrument for chemical warfare and toxic industrial chemical detection; laboratory source for detection of chemical warfare agents; rubber mask for defense against chemicals and gases; chemical composition meter; flowmeters; stirrer; industrial engines; and a buried pipeline locator device. This case resulted from an investigation conducted by OEE's New York Field Office and ICE.

**The Penalty:** On October 25, 2016, Deri was sentenced in U.S. District Court for the Middle District of Pennsylvania to 37 months in prison. On October 13, 2016, Harold Rinko was sentenced to time served, 12 months of home confinement, two years of supervised release, and a \$2,500 criminal fine. Deri and Rinko were also ordered to forfeit \$45,698.

## Technoline SAL / Berty Tyloo

---

**The Violation:** On seven occasions between 2009 and 2010, Technoline SAL of Lebanon violated the EAR when it caused, aided and/or abetted export or reexports to Syria of U.S.-origin mass spectrometers, gas chromatographs and consumables, liquid chromatograph-mass spectrometer systems, and liquid chromatograph modules controlled for anti-terrorism reasons. The equipment, manufactured by Agilent



Technologies, Inc., was classified under ECCN 3A999 and valued in total at \$583,109. During the ordering process for each of the transactions, Technoline either falsely identified the ultimate destination of the items as Iraq or Lebanon, or failed to disclose that the ultimate destination was Syria, specifically Syrian Government ministries or entities. In June 2013, Swiss national Berty Tyloo made false or misleading statement to BIS during the course of the investigation. As early as 2001, Tyloo was the area sales manager or distribution channel manager for the Middle East and Africa for Agilent products for European subsidiaries or affiliates of Agilent. Tyloo stated during an interview that he had "no idea" how products had ended up in Syria, and that, as far as

he knew, all such products had stayed in Lebanon. Similarly, when asked if Technoline had ever shipped U.S.-origin items to Syria, Tyloo stated "No, not to my knowledge." At the time he made these statements, Tyloo knew they were false or misleading and, that in fact, Technoline had sold and distributed items to Syria beginning in at least 2004. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On September 24, 2016, BIS issued Final Orders against Technoline imposing a civil penalty of \$450,000, \$275,000 of which was suspended provided no violations occur during a two-year probationary period. The company also agreed to a two-year denial of export privileges. On January 10, 2017, BIS issued Final Orders against Tyloo imposing a three-year denial of export privileges.

## Fokker Services, B.V.

---

**The Violation:** Between July 2005 and September 2010, Netherlands-based aerospace services provider Fokker Services B.V. (“FSBV”) repeatedly engaged in illegal transactions involving the export and reexport of aircraft parts, technology, and services to Iran and Sudan, while fully aware, including the company’s senior management and its legal and compliance departments, of the applicability of U.S. export control laws, including the EAR. The knowing and willful violations included FSBV’s sale and transfer to and servicing for end users in Iran, including Iranian military end users, of parts and components used in aircraft avionics and navigation systems and in engine, communications, and other aircraft systems, as well as other parts and components. FSBV used a number of schemes, or “work-arounds,” to evade U.S. export control laws and avoid detection by U.S. law enforcement authorities. FSBV, for example, concealed material information from its vendors and suppliers in the United States (and the United Kingdom), including by stripping identifying information associated with Iranian aircraft from items and packaging before sending the parts to repair shops, providing repair shops with false tail numbers, and providing false end user or ownership information, including with regard to transactions involving Iran Air. Other “work-arounds” included using a “black list” that tracked which U.S. companies were more likely to ask for end-user statements or ask questions about the origin of parts, and directing business to other U.S. companies, and inserting an automatic electronic alert notice into an internal database that reminded employees to withhold information about Iranian end users from repair shops and suppliers. BIS alleged that Fokker committed 253 violations of the EAR, including 96 violations for engaging in transactions with Iran Air contrary to the terms of a BIS Temporary Denial Order. These 253 transactions involved items classified under ECCNs 1A001, 7A103, 6A998, 7A994, and 9A991, controlled on missile technology, national security, and anti-terrorism grounds, and valued in total at approximately \$10.7 million. This case resulted from a multi - year investigation led by OEE’s Boston Field Office, OFAC, the FBI, ICE and DCIS, and the U.S. Attorney’s Office for the District of Columbia.

**The Penalty:** On June 2, 2016, the Assistant Secretary approved a settlement agreement under which FSBV agreed to pay a civil penalty of \$10,500,000. FSBV also accepted responsibility for its criminal conduct in violating the IEEPA entered into a deferred prosecution agreement with the Department of Justice. As part of that agreement, FSBV also paid \$10,500,000 to satisfy a forfeiture obligation.

## Amin Al-Baroudi

---

**The Violation:** Amin Al-Baroudi exported military and tactical items and other equipment to supply and arm Ahrar al-Sham and other rebel groups in Syria with U.S.-origin goods. Through this conspiracy, Al-Baroudi illegally exported a variety of items for use on the battlefield, including rifle scopes, night vision rifle scopes and sighting devices, body armor, voltage power meters, range finders, communications equipment, and laser boresighters. On January 15, 2016, Al-Baroudi pled guilty to conspiracy to violate the IEEPA and U.S. sanctions against Syria. This case resulted from a joint investigation conducted by OEE’s Washington Field Office and the FBI.

**The Penalty:** On June 10, 2016, Amin Al-Baroudi was sentenced in U.S. District Court for the Eastern District of Virginia to 32 months in prison (with credit for approximately six months of time served), two years of supervised release, and a \$100 special assessment. Al-Baroudi was also required by the court to forfeit a variety of firearms and other items seized by the U.S. Government during a search warrant executed in connection with this investigation.

## Oguzhan Aydin

---

**The Violation:** On October 13, 2015, Turkish national Oguzhan Aydin pled guilty in U.S. District Court for the Northern District of Georgia in connection with the attempted procurement of F-14 fighter jet parts and C-130 parts for final delivery to Iran via Turkey. Aydin paid approximately \$40,000 as a down payment for the



purchase of the parts. In August 2014, Aydin was arrested upon his arrival to the United States in Houston, Texas and extradited to the Northern District of Georgia. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office and ICE.

**The Penalty:** On March 30, 2016, Aydin was sentenced to 30 months in prison, five years of supervised release, and a \$25,000 criminal fine.

## **Ali Reza Parsa / Metal PM**

---

**The Violation:** Ali Reza Parsa, a Canadian-Iranian dual citizen and resident of Canada, conspired to obtain high- tech electronic components from American companies for transshipment to Iran and other countries for clients of Parsa's procurement company in Iran, Tavan Payesh Mad. Parsa used his Canadian company, Metal PM, to place orders with U.S. suppliers and had the parts shipped to him in Canada or to a freight forwarder located in the United Arab Emirates. He then transshipped from these locations to Iran or to the location of his Iranian company's client. Parsa provided the U.S. companies with false destination and end -user information for the components in order to conceal the illegality of these transactions. In addition, following his arrest and while incarcerated, Parsa continued to violate the IEEPA by conducting business for Metal PM and Tavan Payesh Mad, including by ordering parts from German and Brazilian companies for Iranian customers. Parsa also directed a relative to delete email evidence of his ongoing business transactions while in jail, emphasizing the need for secrecy in their dealings. This case resulted from a joint investigation conducted by OEE's New York Field Office and the FBI.

**The Penalty:** On May 20, 2016, Ali Reza Parsa was sentenced in U.S. District Court for the Southern District of New York to 36 months in prison and a \$300 special assessment.

## **Sihai Cheng**

---

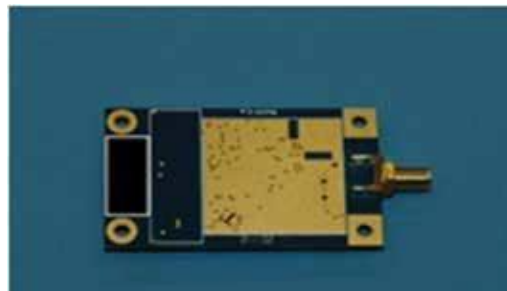
**The Violation:** In 2013, Chinese national Sihai Cheng was charged in an indictment along with Seyed Abolfazl Shahab Jamili, an Iranian national, and two Iranian companies, Nicaro Eng. Co., Ltd. and Eyvaz Technic Manufacturing Company, with conspiring to export, and exporting, highly sensitive U.S.-manufactured goods with nuclear applications to Iran from at least 2009 to 2012. In December 2014, Cheng was extradited from the United Kingdom to the United States and has remained in custody since then. On December 18, 2015, Cheng pled guilty to conspiracy to commit export violations and smuggle goods from the United States to Iran and to illegally exporting U.S.-manufactured pressure transducers to Iran. From February 2009 through at least 2012, Cheng, Jamili, and a third individual conspired with each other and others in China and Iran to illegally obtain hundreds of U.S.-manufactured pressure transducers and export them to Iran. Initially, the parts were exported to China using fraudulently obtained BIS export licenses. When they arrived in the China, Cheng inspected them in the Shanghai Free Trade Zone and removed their U.S. manufacturer serial numbers to conceal the fact that he was violating U.S. law. Cheng then caused the pressure transducers to be exported to Iran knowing that the parts were being supplied to the Government of Iran. Jamili advised Cheng that the Iranian end- user was Kalaye Electronic Company, which the U.S. Government designated as a proliferator of weapons of mass destruction in 2007 for its work with Iran's nuclear centrifuge program. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons -grade uranium. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI and ICE.

**The Penalty:** On January 27, 2016, Cheng was sentenced in U.S. District Court for the District of Massachusetts to nine years in prison and a \$600 special assessment in connection with the export of the pressure transducers to Iran.

## Corezing International Pte., Ltd.

---

**The Violation:** Between 2007 and 2008, Singapore-based Corezing International Pte., Ltd. (Corezing) conspired to illegally export thousands of radio frequency (RF) modules through Singapore to Iran, at least 16 of which were later found in remote detonation systems of unexploded improvised explosive devices (IEDs) in Iraq. Corezing procured RF modules from a U.S. module manufacturer, and sent the modules to a freight forwarder in Singapore in five partial shipments. Shipping documents provided by Singapore Customs showed that once the radio parts were delivered to Singapore, they were transhipped from Singapore to Paya Electronics Complex in Iran. RF modules are classified under ECCN 5A002 and require a license to Iran. On September 15, 2010, five individuals and four of their companies were indicted on a variety of charges, including illegal export of goods from the United States to Iran and the export of military antennas to Singapore. In October 2011, four of the targets were arrested by Singapore Authorities at the request of the United States. These individuals remained in custody while awaiting extradition. On December 21, 2012, two of the four targets were extradited to the United States on charges related to the export of military antennas to Singapore. In October 2014, one of the targets was arrested in Indonesia by Indonesian Authorities at the request of the United States. On April 27, 2017, that target was extradited to the United States based on charges related to the export of the RF modules to Iran. This case resulted from a joint investigation conducted by OEE's Chicago and Boston Field Offices, the FBI and ICE.



*RF Modules like the one pictured here are ordinarily used in wireless local area networks, have encryption capability, and can transmit data wirelessly up to 40 miles when configured with certain antennas.*

**The Penalty:** Ultimately, three individuals, Lim Kow Seng, Hia Soo Gan Benson, and Lim Yong Nam, pled guilty to charges in the District of Columbia. On September 20, 2013, Lim Kow Seng was sentenced to 37 months in prison and three years of supervised release, and Hia Soon Gan Benson was sentenced to 34 months in prison and three years of supervised release. On April 27, 2017, Lim Yong Nam was sentenced to 40 months in prison and two years of supervised release. In November 2018, the United States Department of State's Transnational Organized Crime Rewards Program issued a \$3 million reward for information leading to the arrest and/or conviction of one of the targets in the September 2010 indictment. This target, Hossein Ahmad Larijani, remains at-large in Iran and is associated with the Iranian company (Paya Electronics Complex) that received the RF modules. In addition, BIS announced the addition of 15 persons located in China, Hong Kong, Iran, and Singapore to the BIS Entity List in connection with the investigation and prosecution of Corezing. Their placement on the BIS Entity List prohibits these companies from receiving any item subject to the EAR unless the exporter obtains a BIS license.

## Antennas and Components / Eric Schneider

---

**The Violation:** This investigation was part of the Corezing investigation detailed above. In January 2010, Eric Schneider, principal of Antennas and Components of Andover, Massachusetts, pled guilty to conspiracy in connection with the export of antennas to end users in Singapore and Hong Kong without the required BIS license. The antennas, controlled for export as defense articles, were ultimately shipped to Iran. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI and ICE.

**The Penalty:** On December 15, 2015, Eric Schneider was sentenced in U.S. District Court for the District of Columbia to time served in prison, one year of probation, 500 hours of community service, and a \$100 special assessment.

**The Violation:** During the course of the RH International et al investigation summarized above, Special Agents discovered that Springworks Sdn Bhd of Malaysia was supplying U.S.-origin computer storage hardware and related software items classified under ECCNs 5A002 and 5D002 to Iran via Malaysia and the United Arab Emirates. In January 2015, Kenneth Wei Xian Chua and Chen Chee Onn, also known as Owen Chen, were successfully lured from Malaysia to the Middle District of Florida where they were successfully recorded over a six-day period meeting numerous times with Special Agents posing in an undercover capacity as suppliers of the computer equipment. In January 2015, both Chua and Chen were arrested and successfully interrogated by Special Agents. On August 6, 2015, Chua pled guilty to smuggling in connection with these transactions. On July 30, 2015, Chen pled guilty to charges related to the same transactions. This case resulted from a joint investigation conducted by OEE's Miami Field Office and ICE.

**The Penalty:** On November 10, 2015, Chua was sentenced to two months in prison, three years of probation, a \$3,500 criminal fine, DNA collection, and surrender for deportation upon release to Malaysia with no re-entry to the United States. On November 9, 2015, Chen was sentenced in U.S. District Court for the Middle District of Florida to one year and one day in prison, three years of supervised release, a \$10,000 criminal fine, a \$100 special assessment, and deportation upon release to Malaysia with no re-entry to the United States. The investigation also resulted in a forfeiture of \$ 324,733, the deemed illegal proceeds which were wired as down payments for various orders placed by Chen.

## Barracuda Networks, Inc. and Barracuda Networks, Ltd.

---

**The Violation:** Beginning in April 2009 and continuing through May 2012, Barracuda Networks, Inc. of Campbell, California (Barracuda), and its wholly-owned subsidiary, Barracuda Networks, Ltd. of the United Kingdom (Barracuda UK), engaged in unlicensed export and reexport of U.S.-origin equipment and software to Iran, Syria and Sudan. On 26 occasions Barracuda acted with knowledge of a violation of the EAR by selling or servicing U.S.-origin devices and related software to the sanctioned destinations of Syria, Iran and Sudan. The commodities exported by Barracuda consisted of web filters, firewall products, link balancers and server backup software. On 11 occasions Barracuda UK acted with knowledge of a violation of the EAR by selling or servicing U.S.-origin devices and related software to Syria and Iran with knowledge that a violation would occur. The illegally exported items are controlled by the Commerce Department for national security and/or anti-terrorism reasons and as encryption items. Iran, Syria and Sudan are designated as State Sponsors of Terrorism. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On November 23, 2015, Barracuda Networks Inc. and Barracuda Networks Ltd. agreed to pay a civil penalty of \$1,500,000.

**Voluntary Self-Disclosure:** Barracuda Networks voluntarily disclosed the violations and cooperated fully with the investigation.

## EgyptAir Airlines Company

---

**The Violation:** EgyptAir Airlines Company, the flag carrier airline of Egypt, leased two Boeing 737 commercial aircraft classified under ECCN 9A991 and controlled for anti-terrorism reasons, to Sudan Airways, causing the reexport of the aircraft to Sudan. During the lease, the aircraft were placed under the operational control of Sudan Airways and the operating conditions did not satisfy the criteria for "temporary sojourn" license exception under section 740.15 "Aircraft and Vessels (AVS)" of the EAR. EgyptAir was informed by a third party during the course of the transaction that a license was required for the lease. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On November 17, 2015, EgyptAir agreed to pay a civil penalty of \$140,000.

**Voluntary Self-Disclosure:** EgyptAir voluntarily disclosed the violations and cooperated fully with the investigation.

## Mozaffar Khazaei

---

**The Violation:** From at least 2009 to 2013, Mozaffar Khazaei, a dual citizen of Iran and the United States, stole highly sensitive, proprietary, trade secret and export-controlled material relating to U.S. military jet engines from multiple U.S. defense contractor employees with the intent to send them to Iran. The hard copy and electronic material that Khazaei stole and sought to transfer to Iran totaled some 50,000 pages and was reviewed by experts from both the U.S. Air Force and the victim defense contractors. In addition to materials relating to the JSF Program and the F-22 Raptor, Khazaei also had documents from numerous other U.S. military engine programs, including the V-22 Osprey, the C-130J Hercules and the Global Hawk engine programs. In total, Khazaei sought to export approximately 1,500 documents containing trade secrets and approximately 600 documents containing highly sensitive defense technology. Analysis of Khazaei's computer media also revealed cover letters and application documents which he sent to multiple state-controlled technical universities in Iran. In those materials, Khazaei stated that as "lead engineer" in various projects with U.S. defense contractors, he had learned "key technique[s] that could be transferred to our own industry and universities." In January 2014, Khazaei was arrested at the Newark Liberty International Airport before boarding a flight to return to Iran. Search warrants executed on Khazaei's luggage revealed additional hard copy documents and computer media containing sensitive, proprietary, trade secret and export controlled documents relating to U.S. military jet engines. Khazaei was also found in the possession of \$59,945 in as-yet undeclared cash, which he had split up into increments of approximately \$5,000 and secreted in multiple bank envelopes in various places in his carry-on luggage. Khazaei pled guilty in February 2015. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, ICE, DCIS, U.S. Air Force Office of Special Investigation (AFOSI), and U.S. Customs and Border Protection (CBP).

**The Penalty:** On October 23, 2015, Khazaei was sentenced to 97 months in prison, three years of supervised release, a \$50,000 criminal fine, and a \$100 special assessment.

## Schlumberger Oilfield Holdings Ltd.

---

**The Violation:** Starting in about 2004 and continuing through June 2010, Drilling & Measurements (D&M), a United States-based Schlumberger business segment, provided oilfield services to Schlumberger customers in Iran and Sudan through their non-U.S. subsidiary Schlumberger Oilfield Holdings Ltd. (SOHL), incorporated in the British Virgin Islands. Although SOHL and the parent company Schlumberger Limited had policies and procedures designed to ensure that D&M did not violate U.S. sanctions, both companies failed to train their employees adequately to ensure that all U.S. persons, including non-U.S. citizens who resided in the United States while employed at D&M, complied with Schlumberger Ltd.'s sanctions policies and compliance procedures. As a result of D&M's lack of adherence to U.S. sanctions combined with SOHL's failure to properly train U.S. persons and to enforce fully its policies and procedures, D&M, through the acts of employees residing in the United States, violated U.S. sanctions against Iran and Sudan by: (1) approving and disguising the company's capital expenditure requests from Iran and Sudan for the manufacture of new oilfield drilling tools and for the spending of money for certain company purchases; (2) making and implementing business decisions specifically concerning Iran and Sudan; and (3) providing certain technical services and expertise in order to troubleshoot mechanical failures and to sustain expensive drilling tools and related equipment in Iran and Sudan. This case resulted from an investigation conducted by OEE's Dallas Field Office.

**The Penalty:** In May 2015, Schlumberger Oilfield Holdings Ltd. entered a plea of guilty in U.S. District Court for the District of Columbia and agreed to pay over \$232.7 million, the largest criminal fine ever imposed for violations of sanctions programs administered under the IEEPA. Parent company Schlumberger Ltd. also agreed to the following additional terms during the three-year term of probation maintaining its cessation of all operations in Iran and Sudan, (2) reporting on the parent company's compliance with sanctions regulations, (3) responding to requests to disclose information and materials related to the parent company's compliance with U.S. sanctions laws when requested by U.S. authorities, and (4) hiring an independent consultant to review the parent company's internal sanctions policies and procedures and the parent company's internal audits focused on sanctions compliance.

On June 21, 2016, the OEE Special Agent responsible for this investigation was recognized at the United States Attorney's Office, District of Columbia's Thirty-Fourth Law Enforcement Awards Ceremony for his outstanding work on this case.

## Borna "Brad" Faizy / Touraj Ghavidel / Techonweb

---

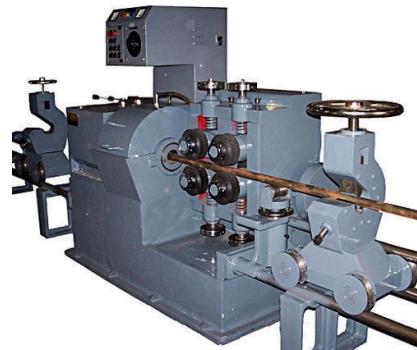
**The Violation:** On October 16, 2014, Borna "Brad" Faizy and Touraj Ghavidel (aka Brent Dell), owners/operators of Signal Microsystems (aka Techonweb) of Addison, Texas, pled guilty to making false statements to federal agents in connection with the export of computers and computer equipment to Iran through the United Arab Emirates. The computers, valued at approximately \$20 million, were classified under ECCN 5A992 for anti-terrorism reasons. As part of their conspiracy, Faizy and Ghavidel acquired computers from U.S. companies to supply to end users in Iran and concealed from the U.S. Government that the computers were destined for Iran. Faizy and Ghavidel actively recruited Iranian customers by marketing their computer business to business owners and individuals in Iran, and, in 2008 or 2009, attended a computer trade show, known as "GITEX," in Dubai to recruit Iranian customers. The defendants used 'General Trading' companies in Dubai to ship the equipment to Iran and communicated with co-conspirators using fictitious names and coded language to obscure the true identities and locations of the ultimate consignees and end users. They also created invoices and export forms that falsely identified the ultimate consignees of the shipments as parties in Dubai. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, the FBI, ICE and DCIS.

**The Penalty:** On April 3, 2015, Faizy and Dell were each sentenced in U.S. District Court for the Northern District of Texas to a \$75,000 criminal fine, two years of probation, and a \$100 assessment, and forfeiture of computer equipment valued at \$425,000. A ten-year denial of export privileges was also placed on both Faizy and Dell.

## Hetran, Inc. / Helmut Oertmann / FIMCO FZE

---

**The Violation:** This case involves a conspiracy to export a bar peeling machine and related parts valued at more than \$800,000 from the United States through the United Arab Emirates to Iran in violation of the Iran embargo. The machine may be used in the production of high grade steel, a product used in the manufacture of aircraft parts. Around June 2009, Hetran, Inc. of Orwigsburg, Pennsylvania (Hetran), was contacted by representatives of Falcon Instrumentation and Machinery FZE, formerly known as FIMCO FZE (FIMCO), an Iranian company with offices in Iran and the United Arab Emirates, regarding the manufacture and purchase of a peeling machine for ultimate shipment to Iran. In furtherance of the conspiracy, Hetran, its President, Helmut Oertmann (Oertmann), and other co-conspirators agreed that the shipping documents would falsely identify Crescent International Trade and Services FZE in Dubai, United Arab Emirates, as the machine's end user. In June 2012, Hetran attempted to export the machine through Dubai to Iran without the required U.S. Government authorization. On May 20, 2014, Hetran and Oertmann each entered a guilty plea in U.S. District Court for the Middle District of Pennsylvania. Hetran pled guilty to conspiracy to violate IEEPA, and Oertmann pled guilty to attempt to smuggle goods from the United States. On July 24, 2015, in U.S. District Court for the Middle District of Pennsylvania, FIMCO also pled guilty to charges of conspiracy to violate IEEPA. The other indicted company, Crescent International Trade and Services FZE, and the three Iranian individuals who served as officers of FIMCO, Khosrow Kasraei, Reza Ghoreishi, and Mujahid Ali, are presently fugitives. This case resulted from an investigation conducted by OEE's New York Field Office.



**The Penalty:** On December 3, 2014, Oertmann and Hetran were each sentenced to 12 months of probation and a \$100 assessment. On the same date, they agreed to be held jointly and severally liable for a civil penalty of \$837,500 in OEE's related administrative conspiracy case. BIS suspended \$500,000 of this penalty for two years and will waive the suspended penalty amount thereafter if the respondents do not commit additional



violations of the EAR during the two-year probationary period. On January 6, 2016, FIMCO was sentenced to a \$100,000 criminal fine and a \$400 special assessment. On July 27, 2015, FIMCO agreed to pay an \$837,500 civil penalty. BIS suspended \$250,000 of this penalty for two years and will waive the suspended penalty amount thereafter if the respondent does not commit additional violations of the EAR during the two -year probationary period. On the same date, BIS issued a two-year suspended denial order against FIMCO.

### **Ya Qian “Jonathan” Chen / SKS Hydraulics USA, Inc.**

---

**The Violation:** Ya Qian Chen, aka Jonathan Chen, pled guilty in June 2014 in connection with the attempted export of helium leak detectors to Iran via China and Hong Kong. Chen, a Chinese national and president of SKS Hydraulics USA, Inc. in Henderson, Nevada, was arrested in June 2014. The leak detectors, classified under ECCN 3A999 and controlled for anti-terrorism reasons, are a critical piece in the uranium enrichment process. This case resulted from a joint investigation conducted by OEE’s Los Angeles Field Office and the FBI.

**The Penalty:** On October 14, 2014, Chen was sentenced to three years of probation, forfeiture of equipment valued at \$19,665, and a \$100 assessment.

### **Trans Merits Co., Ltd.**

---

**The Violation:** Alex Tsai and his former company, Trans Merits of Taiwan, appear on the Office of Foreign Assets Control’s (OFAC) List of Specially Designated Nationals (SDN). Alex Tsai was designated for providing, or attempting to provide, financial, technological, or other support for, or goods or services in support of the Korea Mining Development Trading Corporation (KOMID), which was designated as a proliferator in June 2005. A former resident of Taiwan, Alex Tsai was arrested in May 2013 in Estonia and was later extradited to the United States. Tsai is associated with at least three companies based in Taiwan – Global Interface Company, Inc., Trans Merits Co., Ltd., and Trans Multi Mechanics Co., Ltd. – that purchased and then exported, and attempted to purchase and then export, from the United States and other countries, machinery used to fabricate metals and other materials with a high degree of precision. This case resulted from a joint investigation conducted by OEE’s Chicago Field Office, the FBI and ICE.

**The Penalty:** On October 10, 2014 and December 16, 2014, Alex Tsai and his son Gary Tsai, respectively, pled guilty in connection with each of their roles in a scheme for Gary Tsai to illegally export milling machines to his father, Alex Tsai. On April 23, 2015, Gary Tsai was sentenced in U.S. District Court for the Northern District of Illinois to three years of probation, a \$250 criminal fine and a \$100 special assessment. On March 16, 2015, Alex Tsai was sentenced to two years of prison and a \$100 special assessment.

### **Mohammad Reza Hajian / RH International LLC / Nexiant LLC/ P & P Computers LLC / Randy Barber / Michael Dragoni / Fortis Data Systems LLC / Greencloud LLC / John Talley / Tallyho Peripherals, Inc.**

---

**The Violation:** OEE has been conducting an ongoing, multi-year investigation involving the illegal export of high-end computers, software, data storage arrays, and equipment to Iran. Mohammad Reza “Ray” Hajian, Randy Dale Barber, Michael Dragoni, and John Alexander Talley conspired to export sophisticated computer and related equipment classified under numerous ECCNs including 4A994, 5A002, 5A991, 5A992, and 5D992 from the United States to Iran, in violation of the U.S. embargo. Dragoni and Barber, using Dragoni’s companies Fortis Data Systems LLC (FDS) and Greencloud LLC, conspired to defraud Hitachi Data Systems (HDS) by making materially false statements to HDS in order to purchase computer equipment for resale to Hajian, who in turn resold the equipment to his client, a UAE



company. By late 2009, Dragoni, Barber and Hajian knew that HDS refused to sell computer equipment to Hajian and his customers because HDS believed that the equipment was being diverted to unauthorized end users. In order to deceive HDS and purchase the computer equipment, Dragoni and Barber made false statements regarding the purchaser, end user, and location of installation of the equipment that they were purchasing. To facilitate the conspiracy, they used front companies to make equipment purchases on their behalf. The conspirators then caused the equipment to be shipped to Dubai. Talley's role was to provide training and computer IT support to ensure that the computer equipment operated in Iran. In an effort to conceal their activities, the conspirators in the United States caused shipments of the computers and related equipment, as well as the payments for same, to travel to and from the United States and Iran through the UAE. Similarly, payments for Talley's support services were wired through the UAE. This case resulted from a joint investigation conducted by OEE's Miami Field Office and ICE.

**The Penalty:** In July 2014, Randy Dale Barber was sentenced to five years of probation, a forfeiture of \$413,106 and (joint) restitution in the amount of \$37,921 to HDS. Michael Dragoni was sentenced to five years of probation, with eight months of home detention, in addition to the joint restitution. FDS and Greencloud were each sentenced to five years of probation. In addition, Dragoni, FDS and Greencloud were sentenced to a joint forfeiture of \$498,706 and the joint restitution with Barber to HDS. In April 2014, John Alexander Talley was sentenced to 30 months in prison and his company, Tallyho Peripherals, Inc., doing business as Enterprise Solutions Systems, was sentenced to one year of probation. In October 2012, Hajian was sentenced to four years in prison, one year of supervised release, and a (shared) forfeiture of \$10 million (the traceable proceeds of the offense), and a \$100 assessment. Hajian's companies, RH International, P&P Computers LLC, and Nexiant LLC were each sentenced to 12 months of probation, a \$400 assessment, and the shared \$10 million forfeiture. On March 22, 2013, BIS issued Final Orders against Hajian and each of his three companies imposing a 10-year denial of export privileges.

### **Computerlinks FZCO / Infotec / Waseem Jawad / Aramex Emirates LLC**

---

**The Violation:** Computerlinks FZCO, the United Arab Emirates subsidiary of the German firm Computerlinks AG, committed three violations of the EAR related to the transfer to Syria of Blue Coat devices designed for use in monitoring and controlling internet traffic. Computerlinks, at the time an authorized reseller for Blue Coat Systems, Inc. of Sunnyvale, California, ordered Blue Coat equipment valued at approximately \$1.4 million, which is classified as ECCN 5A002 and 5D002 and controlled for national security and anti-terrorism reasons and as encryption items. Computerlinks FZCO provided Blue Coat, the U.S. manufacturer and exporter, with false information concerning the end user and ultimate destination of the items in connection with these transactions. Computerlinks FZCO knew that the items were destined for end users in Syria. However, when placing these orders with Blue Coat, Computerlinks FZCO falsely stated that the ultimate destination and end users for the items was the Iraq Ministry of Telecom (on two occasions) or the Afghan Internet service provider Liwalnet (on one occasion). The items subsequently were shipped to Computerlinks FZCO in the UAE for ultimate delivery to Syria without the required licenses having been obtained. BIS also identified Waseem Jawad, using the company name Infotec, as a middleman between Computerlinks FZCO and the Syrian end users, as well as freight forwarder Aramex Emirates LLC, located in Dubai. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On May 8, 2014, Aramex Emirates LLC agreed to pay \$125,000 in civil penalties. On April 24, 2013, Computerlinks FZCO agreed to pay a \$2,800,000 civil penalty, the statutory maximum and complete three external audits of its export control compliance program. "Today's settlement reflects the serious consequences that result when companies take actions to evade U.S. export controls and is the result of an aggressive investigation by OEE and prosecution by the Office of Chief Counsel for Industry and Security of the unlawful diversion of U.S.-origin technology to Syria," said Under Secretary for Industry and Security Eric L. Hirschhorn. "It is vital that we keep technology that can be used to further the repression of the Syrian people out of the hands of the Syrian government." On December 16, 2011, BIS added Waseem Jawad and Infotec to the BIS Entity List in connection with the investigation into Computerlinks FZCO.

## Weatherford International

---

**The Violation:** From 1998 through 2007, Weatherford International and four of its subsidiaries, Weatherford Oil Tools Middle East, Weatherford Production Optimization (UK) Limited, Precision Energy Services ULC (Canada) and Precision Energy Services Columbia Limited, engaged in conduct that violated various U.S. export control and sanctions laws by exporting or reexporting EAR99 oil and gas drilling equipment to, and conducting Weatherford business operations in, sanctioned countries without the required U.S. government authorization. In addition to the involvement of employees of several Weatherford International subsidiaries, some Weatherford International executives, managers or employees on multiple occasions participated in, directed, approved and facilitated the transactions and the conduct of its various subsidiaries. This conduct involved persons within the U.S.-based management structure of Weatherford International participating in conduct by Weatherford International foreign subsidiaries and the unlicensed export or reexport of U.S.-origin goods to Cuba, Iran, Sudan and Syria. Weatherford subsidiaries Precision Energy Services Colombia Ltd. and Precision Energy Services ULC fka Precision Energy Services Ltd., both headquartered in Canada, conducted business in Cuba. Weatherford's subsidiary Weatherford Oil Tools Middle East, headquartered in the United Arab Emirates, conducted business in Iran, Sudan and Syria. Weatherford's subsidiary Weatherford Production Optimisation (UK) Limited fka eProduction Solutions U.K. Ltd., headquartered in the United Kingdom, conducted business in Iran. Combined, Weatherford generated approximately \$110 million in revenue from its illegal transactions in Cuba, Iran, Syria and Sudan. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, the FBI, ICE, the Department of Treasury's Office of Foreign Assets Control, the U.S. Securities and Exchange Commission, the U.S. Department of Justice, and the Houston Police Department.

**The Penalty:** On November 26, 2013, Weatherford International agreed to enter into a deferred prosecution agreement for a term of two years, and two of its subsidiaries agreed to plead guilty to export controls violations under the IEEPA and the Trading With the Enemy Act. Weatherford and its subsidiaries also agreed to pay a penalty of \$100 million, with a \$48 million penalty paid pursuant to the deferred prosecution agreement, \$2 million paid in criminal fines pursuant to the two guilty pleas, and a \$50 million civil penalty paid to resolve the violations charged by BIS. Weatherford International and some of its affiliates also signed a \$91 million settlement agreement with the Department of the Treasury, Office for Foreign Assets Control to resolve their civil liability arising out of this same conduct, which will be deemed satisfied by the payment of the \$100 million in penalties mentioned above. In conjunction with the sanctions settlement, Weatherford International agreed to enter into an additional deferred prosecution agreement for a term of two years and one of its subsidiaries has agreed to plead guilty for violations of the Foreign Corrupt Practices Act. This agreement included an additional \$87.2 million criminal penalty and \$65.6 million in civil fines to the Securities and Exchange Commission.

**This massive seven year joint investigation resulted in the conviction of three Weatherford subsidiaries, the entry by Weatherford International into two deferred prosecution agreements, multiple civil settlement and payment of a total of \$252,690,606 in penalties and fines.**

## Mahan Airways and Balli Group PLC

---

**The Violation:** Between 2005 and 2008, Balli Group PLC and its related companies and individuals (known collectively as Balli) conspired with Iranian airline Mahan Air to export or re-export U.S.-origin Boeing 747 aircraft to Iran without the required U.S. Government authorization. Three of the aircraft were flying on routes in and out of Iran using Iranian flight numbers while under the operational control of Mahan Air. On March 21, 2008, BIS issued a Temporary Denial Order (TDO) lasting 180 days and suspending the export privileges of Balli, Blue Airways (Armenia), and Mahan Air (Iran), based on evidence that the parties knowingly re-exported three U.S.-origin aircraft to Iran and were preparing to re-export three additional U.S.-origin aircraft to Iran without the required export license or authorization. From July to September 2008, Balli conducted negotiations with persons, including another person subject to the TDO, concerning financing, receiving and/or using the U.S.-origin aircraft. Balli allowed the aircraft to continue operation contrary to U.S. export control laws, despite warnings from BIS and

the manufacturer. Balli also concealed information regarding the ultimate destination, end user, and the role the Iranian airline played in the acquisition and financing of the aircraft via funds from the Iranian Foreign Exchange Reserve Fund. On February 5, 2010, Balli pled guilty to charges related to the illegal export of commercial Boeing 747 aircraft to Iran without the required export license and violating the BIS TDO.

**The Penalty:** On May 11, 2010, Balli was sentenced to pay a \$2 million criminal fine and to serve a five-year corporate period of probation. Additionally, on February 4, 2010, Balli entered a civil settlement with BIS and the Treasury Department's Office of Foreign Assets Control (OFAC) which included a civil penalty of \$15 million, of which \$2 million was suspended and a five-year denial of export privileges that was also suspended pending no future violations and the full and timely payment of the civil penalty. Under the terms of the civil settlement, Balli was also required to submit the results of an independent audit of its export compliance program to BIS and OFAC for each of the next five years. Based on a failure by Balli to make a timely installment payment, BIS issued an order on May 19, 2011 revoking the suspended \$2 million civil penalty and accelerating the due dates for payment on the two remaining installments of the original fine and accelerate payment on the two remaining \$2.6 million installments of the original fine. The Assistant Secretary for Export Enforcement has signed several TDO Renewals against Mahan Air and related parties, the latest being June 5, 2019.



*One of the aircraft exported to Iran by the Balli Group, et al.*

## **Mohammad Tabibi / Michael Edward Todd / Hamid Seifi / Parts Guys LLC / Galaxy Aviation Services**

---

**The Violation:** Mohammad Tabibi, an Iranian national, Michael Edward Todd, owner of The Parts Guys LLC of Perry, Georgia, and Hamid Seifi, an Iranian-born U.S. national and owner of Galaxy Aviation Services in St. Charles, Illinois, were involved in a conspiracy to receive and fill orders for components, including military parts for the Bell AH-1 attack helicopter, the UH-1 Huey attack helicopter, as well as the F-5 and F-4 fighter jets for export to Iran. Fugitive Iranian nationals Hasan and Reza Seifi as well as other indicted co-conspirators located in the United Arab Emirates and France purchased these ITAR and ECCN 9A991 components from Todd and Hamid Seifi on the behalf of parties in Iran and conspired to export the components without obtaining the required U.S. Government licenses. Following his 2011 arrest in the Czech Republic, Tabibi was extradited to the United States and pled guilty. In 2011, Todd, Seifi and Galaxy Aviation pled guilty to charges related to their roles in a conspiracy to violate the Arms Export Control Act and the IEEPA. In June 2011, BIS announced the addition of eight indicted defendants located in France, Iran and the United Arab Emirates to the BIS Entity List. This case resulted from a joint investigation conducted by OEE's Miami Field Office, the FBI and ICE.

**The Penalty:** On December 10, 2013, Tabibi was sentenced to 38 months in prison, a \$200 special assessment and a \$32,000 forfeiture. On June 22, 2011, Seifi was sentenced to 56 months in prison, three years of supervised release, a \$12,500 criminal fine, a \$200 special assessment, and a forfeiture of \$153,940 to be shared with his company Galaxy Aviation Services. On June 22, 2011, Galaxy Aviation Services was sentenced to a \$400 special assessment and the shared \$153,940 forfeiture with Seifi. On October 26, 2011, Todd was sentenced to 46 months in prison, three years of supervised release, and a separate forfeiture (based upon the value of the transactions done by each party) of \$160,362, shared with The Parts Guys, Seifi, and Galaxy Aviation Services. On October 26, 2011, The Parts Guys LLC was sentenced to a \$400 special assessment and the shared \$160,362 forfeiture.

**The Penalty:** On September 17, 2008, 75 additions were made to the BIS Entity List because of the entities' involvement in a global procurement network which began with Mayrow General Trading Company. The Entity List prohibits Mayrow-related companies from receiving any items subject to the EAR unless the exporter secures a BIS license.



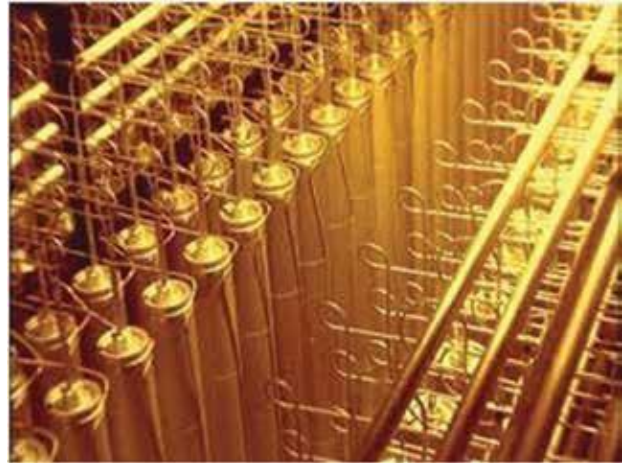
# Chapter 2 – Commerce Control List-Based Controls

## Introduction

The U.S. Government maintains controls on exports of certain items based on its participation in multilateral export control regimes as well as for unilateral foreign policy reasons. These items are identified on the Commerce Control List and controlled pursuant to Part 742 of the EAR.

EAR controls based on multilateral export control regimes include:

- ☐ NP (nuclear nonproliferation) controls implemented pursuant to the Nuclear Suppliers Group. The EAR controls items that could be of significance for nuclear explosive purposes or that will be used, directly or indirectly, in nuclear explosive activities and safeguarded or unsafeguarded nuclear activities;
- ☐ CB (chemical-biological) controls implemented pursuant to the Australia Group. The EAR controls items, including entire chemical plants, toxic chemicals and precursors, and certain microorganisms, that could be used for chemical or biological weapons programs;
- ☐ MT (missile technology) controls implemented pursuant to the Missile Technology Control Regime. The EAR controls unmanned delivery systems, including unmanned aerial vehicles, capable of delivering weapons of mass destruction; and
- ☐ NS (national security) controls implemented pursuant to the Wassenaar Arrangement.



*Gas centrifuges can be used to enrich uranium and are subject to nuclear nonproliferation (NP) controls.*

The EAR controls dual-use and certain military items that could make a significant contribution to the military potential of another country or combination of countries that would prove detrimental to the national security of the United States, including destabilizing accumulations of conventional weapons and military modernization programs.

In addition to these export control regimes, BIS controls items pursuant to multilateral treaties. These include:

- ☐ CW (chemical weapons) controls implemented pursuant to the Chemical Weapons Convention. The EAR controls dual-use chemicals and related technology in addition to CB items that could contribute to chemical weapons programs.
- ☐ FC (Firearms Convention) controls implemented pursuant to the Inter-American Convention Against the Illicit Manufacturing of and Trafficking in Firearms, Ammunition, Explosives, and Other Related Materials (CIFTA). The EAR controls shotguns, shells, optical sights, and other related CIFTA items that could contribute to such activities as drug trafficking, terrorism, and transnational organized crime within the Organization of American States.

BIS also imposes unilateral controls on items in the following categories: significant items (SI), encryption (EI), anti-terrorism (AT), communication intercept/surreptitious listening (SL), regional stability (RS) and crime control and other items for human rights (CC) reasons.

## Criminal and Administrative Case Examples

### *Nuclear Nonproliferation Controls:*

#### **Imran Khan / Kamran Khan / Muhammad Ismail**

---

**The Violation:** From at least December 2012 through December 2016, brothers Imran Khan and Kamran Khan and their father Muhammad Ismail engaged in a scheme to purchase U.S.-origin items, including spectrometers classified under ECCN 3A999 and other commodities designated EAR99, for parties in Pakistan that appear on the BIS Entity List. Through companies conducting business as Brush Locker Tools, Kauser Enterprises-USA and Kauser Enterprises-Pakistan, the three defendants received orders from a Pakistani company that procured materials and equipment for the Pakistani military, requesting them to procure specific products that were subject to the EAR. When U.S. manufacturers asked about the end user for a product, the defendants either informed the manufacturer that the product would remain in the United States, or completed an end-user certificate indicating that the product would not be exported. After the products were purchased, they were shipped by the manufacturer to the defendants in Connecticut. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission (PAEC), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics (NILOP), all of which appeared on the BIS Entity List. The defendants never obtained a BIS license to export any item to the designated entities even though they knew that a license was required prior to export. The defendants received the proceeds for the sale of export-controlled items through wire transactions to a U.S. bank account that the defendants controlled. In June 2017, Imran Khan pled guilty to violating IEEPA when he procured, received, and exported a spectrometer to PAEC without an export license. In March 2018, Muhammad Ismail and Kamran Khan each pled guilty for causing funds to be transferred from Pakistan to the United States in connection with the export control violations. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, ICE, DCIS, and USFIS.

**The Penalty:** On September 19, 2018, Imran Khan was sentenced to three years of probation (the first six months of which were to be served in home confinement), a \$3,000 criminal fine, 100 hours of community service, and a \$200 special assessment. On July 18, 2018, Kamran Khan and Muhammed Ismail were each sentenced to 18 months in prison, three years of probation, and a \$100 special assessment.

#### **MHz Electronics, Inc.**

---

**The Violation:** On two occasions during 2013, MHz Electronics, Inc. of Phoenix, Arizona, violated the EAR when it exported pressure transducers classified under ECCN 2B230 and controlled for nuclear nonproliferation reasons to China and Taiwan without the required BIS export licenses. MHz Electronics, Inc. sold the pressure transducers, which have nuclear explosive applications, through eBay. The company did not have a program in place to ensure its compliance with U.S. export control laws or regulations despite a visit from FBI Special Agents prior to the exports, wherein the Special Agents expressed concern to company officials that a different item MHz Electronics was selling on eBay would have required an export license if shipped to customers outside of the United States. This case resulted from an investigation conducted by OEE's Los Angeles Field Office.

**The Penalty:** On January 11, 2018, MHz Electronics, Inc. agreed to pay a \$10,000 civil penalty, all of which was suspended provided no violations occur during a two-year probationary period. The company was also ordered to complete an external audit of its export compliance program, to be conducted by an unaffiliated third-party consultant.

#### **Fuyi Sun / Zhong Li Bang Ye International Trading Co. Ltd.**

---

**The Violation:** On April 21, 2017, Fuyi "Frank" Sun, a citizen of China, pled guilty to violating the IEEPA in connection with a scheme to illegally export high -grade carbon fiber to China without a license. The carbon fiber, classified under ECCN 1C210, is used primarily in aerospace and military applications. Since approximately 2011,

Sun used fraudulent documents and code words in his attempt to acquire high-grade carbon fiber, including Toray type carbon fiber. On April 11, 2016, Sun traveled from China to New York for the purpose of purchasing carbon fiber from an undercover company. During meetings with undercover agents, Sun repeatedly suggested that the Chinese military was the ultimate end user for the carbon fiber he sought to acquire from the undercover company and claimed to have personally worked in the Chinese missile program. On April 12, 2016, Sun agreed to purchase two cases of carbon fiber from the undercover company. Sun paid the undercover agents \$23,000 in cash for the carbon fiber, as well as an additional \$2,000 as compensation for the risk he believed the undercover company was taking to illegally export the carbon fiber to China without a license. Sun was arrested the next day. This case resulted from a joint investigation conducted by OEE's New York Field Office, ICE, and DCIS.

**The Penalty:** On August 31, 2017, Sun was sentenced in U.S. District Court for the Southern District of New York to three years in prison. On June 13, 2018, BIS issued an order denying Sun's export privileges for ten years (until August 31, 2027).

## **Cryofab, Inc.**

---

**The Violation:** On two occasions during 2012, Cryofab, Inc. of Kenilworth, New Jersey, engaged in conduct prohibited by the EAR by exporting gas storage containers and related tools and accessories designated EAR99 to the Bhabha Atomic Research Center (BARC), without the required BIS export licenses. At the time of the exports, BARC appeared on the BIS Entity List. Although an experienced exporter, Cryofab Inc. failed to screen against the BIS Entity List in connection with these two transactions, and failed to seek or obtain the required BIS export licenses. It also erroneously listed the items as eligible for shipment without a license on the Shipper's Letter of Instructions for each shipment. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On August 18, 2017, Cryofab, Inc. agreed to pay a \$35,000 civil penalty. The company was also ordered to complete an external audit of its export controls compliance program, to be conducted by an unaffiliated third-party consultant.

## **Trexim Corporation / Bilal Ahmed**

---

**The Violation:** On October 2, 2014, Bilal Ahmed pled guilty in connection with the export of carbon fiber and microwave laminates, and the attempted export of a thermal imaging camera, from his company Trexim Corporation of Schaumburg, Illinois, to Pakistan without the required export licenses. Ahmed admitted that in 2009 he shipped carbon fiber to Pakistan's Space and Upper Atmosphere Research Commission (SUPARCO), an entity on the BIS Entity List. Ahmed knew that the carbon fiber and thermal imaging camera were export-restricted and a license was required from the U.S. Government. Ahmed also undervalued the goods he exported to Pakistan to avoid filing an SED and to avoid detection. The carbon fiber was classified under ECCN 1C210 and was controlled for nuclear non-proliferation and anti-terrorism reasons. The thermal imaging camera was classified under ECCN 6A003 and was controlled for national security and regional stability reasons. Ahmed was arrested in March 2014 as he attempted to ship a FLIR thermal imaging camera to Pakistan. This case resulted from a joint investigation conducted by OEE's Headquarters and the FBI.

**The Penalty:** On May 14, 2015, Bilal Ahmed was sentenced in U.S. District Court for the Northern District of Illinois to 24 months in prison, two years of supervised release, a \$1,000 criminal fine, and a \$100 special assessment.

## **Teledyne LeCroy**

---

**The Violation:** On two occasions during 2010, Teledyne LeCroy of Chestnut Ridge, New York, exported oscilloscopes from the United States to the Beihang University of Aeronautics and Astronautics (BUAA), also known as Beihang University, in Beijing, China, without the required BIS export license. BUAA and its Beihang

University alias appeared on the BIS Entity List at the time of the exports. The oscilloscopes were classified under ECCN 3A292 and were controlled for nuclear non-proliferation and/or anti-terrorism reasons. At the time of the transactions, Teledyne LeCroy was aware that BUAA and its Beihang University alias appeared on the BIS Entity List. Teledyne LeCroy had also obtained end-user statements for both exports that listed “Beijing Beihang University” as the end user of the oscilloscope. However, the company failed to properly screen the BIS Entity List connection and failed to obtain the BIS licenses required. Teledyne LeCroy also failed to file accurate Shippers Export Declarations in connection with these transactions. This case resulted from an investigation conducted by OEE’s New York Field Office.

**The Penalty:** On June 16, 2015, Teledyne LeCroy agreed to pay a civil penalty of \$75,000.

## Nicholas Kaiga / IMC Metals Company

---

**The Violation:** On December 4, 2014, Nicholas Kaiga of IMC Metals Company, located in the United Kingdom and Belgium, pled guilty to charges related to his involvement in a scheme to illegally transship aluminum tubing through Belgium to a company in Malaysia. The company in Malaysia was under the control of an individual from Iran. The aluminum tubing is classified as ECCN 1C202 and is controlled for reasons of nuclear nonproliferation. This case resulted from a joint investigation conducted by OEE’s Chicago Field Office, the FBI and ICE.

**The Penalty:** On March 3, 2015, Nicholas Kaiga was sentenced in U.S. District Court for the Northern District of Illinois to 27 months in prison, two years of supervised release (to be conducted outside of the country), and a \$100 special assessment.

## Qiang (Johnson) Hu / MKS Shanghai

---

**The Violation:** This investigation was initiated after photographs surfaced of the former President of Iran, Mahmoud Ahmadinejad, touring the Natanz Uranium Enrichment facility in Iran which revealed the presence of what appeared to be pressure transducers manufactured by MKS Instruments in Andover, MA. From 2008 through his arrest in 2012, Qiang (Johnson) Hu, a sales manager at MKS Shanghai, conspired with co-workers and others to illegally supply thousands of export-controlled pressure transducers, worth more than \$6.5 million, to unauthorized end users in China, Iran and elsewhere using export licenses fraudulently obtained from the Department of Commerce. The pressure transducers are classified under ECCN 2B230 and are controlled for nuclear nonproliferation reasons. Hu was arrested in May 2012 and in October 2013 he pled guilty to conspiracy to violate IEEPA. This case resulted from a joint investigation conducted by OEE’s Boston Field Office, the FBI, and ICE.

**The Penalty:** On July 21, 2014, Hu was sentenced in the U.S. District Court for the District of Massachusetts to 34 months in prison and \$100 special assessment. On February 3, 2016, BIS issued an order denying Hu’s export privileges for ten years (until July 24, 2024).

## Lisong Ma

---

**The Violation:** On May 27, 2013, Lisong Ma, aka Ma Li, a Chinese citizen, pled guilty in connection with the illegal export of weapons - grade carbon fiber to China. Ma attempted to export up to five tons of carbon fiber without the required BIS licenses. The carbon fiber, classified under ECCN 1C210, has applications in the defense and aerospace industries, and was controlled for reasons of nuclear nonproliferation. Ma was arrested in April 2013, in Los Angeles, California, after attempting to acquire the specialized materials. This case resulted from a joint investigation conducted by OEE’s New York Field Office, ICE, and DCIS.

**The Penalty:** On May 24, 2014, Ma was sentenced to 46 months in prison and a \$100 assessment. On October 31, 2014, BIS issued an order denying Ma’s export privileges for a period of ten years (until May 27, 2024).



## Xun Wang / PPG Paints Trading Shanghai / Huaxing Construction

---

**The Violation:** From 2006 through 2007, Chinese companies PPG Paints Trading Shanghai Co Ltd, Huaxing Construction Co Ltd., and Xun Wang, Managing Director of PPG Paints Trading, agreed upon a scheme to export, reexport and transship high-performance epoxy coatings from the United States to Chashma II Nuclear Power Plant in Pakistan. The epoxy coatings, designated as EAR99, were transshipped via a third party in China without having first obtained the required export license. Chashma II is owned by the Pakistan Atomic Energy Commission, which appears on the BIS Entity List. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** In December 2012, Huaxing Construction pled guilty and as part of its plea agreement, agreed to pay the maximum criminal fine of \$2 million, with \$1 million suspended if no further violations occur during the five years of probation. Under the terms of a related civil settlement, Huaxing Construction also agreed to pay another \$1 million, implement an export compliance program, a five-year denial order suspended if no further violations occurring during that period, and be subject to multiple third -party audits over the following five years. Xun Wang also pled guilty and was sentenced to 12 months in prison, a \$100,000 criminal fine, and one year of probation. Under the terms of a related civil settlement, Wang also agreed to pay a civil penalty of \$250,000 (with \$50,000 suspended), and to be placed on the Denied Persons List for a period of ten years with five years suspended. In December 2010, PPG Paints Trading Shanghai pled guilty, and as part of its plea agreement agreed to pay the maximum criminal fine of \$2 million, serve five years of corporate probation, and forfeit \$32,319 to the U.S. Government. Under the terms of a related civil settlement, PPG Paints Trading Shanghai also agreed to pay a civil penalty of \$1 million and complete third-party audits. Huaxing Construction's guilty plea in this case marks the first time a Chinese corporate entity has entered a plea of guilty in a U.S. criminal export matter.

**On September 10, 2014, OEE Special Agents, along with the Assistant U.S. Attorney assigned to the case, were awarded the Executive Office of the U.S. Attorney Director's Award by U.S. Attorney General Eric Holder in recognition of their achievement in the category of Superior Performance by a Litigation Team in connection with this investigation.**

## Nadeem Akhtar / Computer Communication USA

---

**The Violation:** From October 2005 through March 11, 2010, Nadeem Akhtar, owner and operator of Computer Communication USA (CC-USA) of Silver Spring, Maryland, and his co-conspirators used CC-USA to obtain or attempt to obtain radiation detection devices classified under ECCN 1A999, as well as EAR99 resins for coolant water purification, calibration and switching equipment, attenuators and surface refinishing abrasives, mechanical and electrical valves, cranes and scissor lifts for export to entities in Pakistan. Akhtar conspired to send the items to Pakistan's Space and Upper Atmosphere Research Commission (SUPARCO) as well as the Pakistan Atomic Energy Commission (PAEC) and its subordinate entities, such as the Chashma Nuclear Power Plant I in Kundian, Pakistan, and the research reactor maintained by the Pakistan Institute of Engineering and Applied Sciences, a constituent institution of the PAEC specializing in nuclear-related research and development. All of these entities are on the BIS Entity List. The items were worth over \$400,000 total and required export licenses from BIS. Akhtar attempted to evade export regulations and licensing requirements by providing false information, using third parties to procure items for him under false pretenses, misrepresenting CC-USA as the purchaser/end user of the items, and transshipping the items through the United Arab Emirates (UAE). Akhtar took direction and received commissions from the owner of a trading company located in Karachi, Pakistan, regarding what materials were needed and methods to conceal the transactions. Akhtar's co-conspirators included individuals associated with the owner of the Pakistani trading company in Pakistan, Dubai, UAE and New York. The restricted entities were involved in nuclear and energy research and development, nuclear power plants, and applied science. Exports of commodities to these organizations were prohibited without an export license. On September 9, 2011, Akhtar pled guilty in U.S. District Court in the District of Maryland to conspiring to violate the IEEPA and to defraud the United States. This case resulted from a joint investigation conducted by OEE's Washington Field Office and the FBI.

**The Penalty:** On January 6, 2012, Nadeem Akhtar was sentenced to 37 months in prison, two years of supervised release, and a \$100 special assessment.



## **Jirair Avanesian / Farhad Masoumian / Amirhossein Sairafi / XVAC**

---

**The Violation:** Between 2007 and 2008, Jirair Avanesian, the owner and operator of XVAC, in Glendale, California, purchased and exported at least seven shipments of high-dollar vacuum pumps and pump-related equipment classified under ECCN 2B230 to Iran through a free trade zone located in the United Arab Emirates. The vacuum pumps and related equipment have a number of applications, including uranium enrichment. Avanesian purchased the goods on behalf of Farhad Masoumian in Iran, and arranged to ship the goods to the United Arab Emirates, making it appear that the United Arab Emirates was the ultimate destination. Another individual involved in the conspiracy, Amirhossein Sairafi of Iran, would then send the same goods from the location in the United Arab Emirates to Iran. As part of the conspiracy, Masoumian, Avanesian and Sairafi re-labeled and undervalued the contents of the shipments to mask the true contents and to avoid interception by U.S. officials. In most cases, Avanesian prepared air waybills indicating his shipments contained “spare parts” and that no Shipper’s Export Declaration was needed. Avanesian was indicted on December 30, 2009, and arrested in January 2010; he pled guilty in July 2010. Sairafi was arrested in January 2010 in Frankfurt, Germany, by German law enforcement authorities based on a provisional arrest warrant from the United States. Sairafi was extradited to the United States in September 2010, and pled guilty on November 30, 2010. Masoumian remains a fugitive and is believed to be in Iran. This case resulted from a joint investigation conducted by OEE’s Los Angeles Field Office, the FBI, ICE, CBP, and the Internal Revenue Service-Criminal Investigation Division.

**The Penalty:** On July 6, 2011, Avanesian was sentenced to 18 months in prison, three years of supervised release, a \$10,000 criminal fine, and forfeiture of the proceeds of his criminal activity. On September 27, 2012, BIS issued an order denying Avanesian’s export privileges for ten years. In March 2013, Sairafi was sentenced to 41 months in prison.

## **Peter Gromacki / Hamid Reza Hashemi / Amir Abbas Tamimi / Murat Taskiran**

---

**The Violation:** On July 30, 2013, Peter Gromacki, owner and operator of Performance Engineered Nonwovens, located in Middletown, New York, pled guilty to charges of violating IEEPA and conspiracy. On July 10, 2013, Amir Abbas Tamimi, a citizen of Iran, pled guilty to conspiracy and IEEPA violations, and on July 1, 2013, Hamid Reza Hashemi pled guilty to conspiracy and violating IEEPA. On December 5, 2012, the U.S. Attorney’s Office announced charges against Gromacki, Hamid Reza Hashemi and related parties, including Amir Abbas Tamimi and Murat Taskiran, for exporting various goods from the United States to Iran and China without the required export licenses. These goods include carbon fiber classified under ECCN 1C010 and controlled for national security reasons. The carbon fiber has a wide variety of uses, including in gas centrifuges that enrich uranium and in military aircraft and strategic missiles. To evade U.S. restrictions on export of this type of carbon fiber to China, Gromacki enlisted the help of co-conspirators in Europe and China and made false statements on U.S. Customs forms. Hashemi, arrested in December 2012, and Tamimi, arrested in October 2012, were both arrested upon arrival in the United States at JFK International Airport. This case resulted from a joint investigation conducted by OEE’s New York Field Office, the FBI and ICE.

**The Penalty:** On November 26, 2013, Gromacki was sentenced to three months in prison, three years of probation, a \$5,000 criminal fine, and a \$300 special assessment. On November 15, 2013, Hashemi was sentenced to 46 months in prison, one year of probation, and a \$100 special assessment. On November 15, 2013, Tamimi was sentenced to 46 months in prison and a \$100 special assessment. On July 23, 2015, BIS issued an order denying Gromacki’s export privileges for ten years (until November 26, 2023).

## *Chemical/Biological Weapons Controls:*

### **Envirotech Pump Systems, Inc.**

---

**The Violation:** Between 2007 and 2011, Envirotech Pump Systems, Inc. of St. Louis, Missouri, engaged in conduct prohibited by the EAR on 32 occasions by exporting globe, gate or butterfly valves valued at approximately \$1.4 million to China, Russia, and other various destinations without the required BIS export licenses. These items were classified under ECCN 2B350 and were controlled for reasons of chemical and biological weapons proliferation. This case resulted from an investigation conducted by OEE's Chicago Field Office.

**The Penalty:** On July 22, 2015, Envirotech Pump Systems, Inc. agreed to pay a civil penalty of \$500,000 with \$350,000 suspended provided no violations occur during a two-year probationary period. The company also agreed to complete two audits of its export controls compliance program.

**Voluntary Self-Disclosure:** Envirotech Pump Systems, Inc. voluntarily disclosed the violations and cooperated fully with the investigation.

### **Flowserve Corporation**

---

**The Violation:** Between 2002 and 2008, Flowserve Corporation, located in Irving, Texas, and ten of its foreign affiliates made unlicensed exports and reexports of pumps, valves and related components classified under ECCN 2B350 to a variety of countries including China, Singapore, Malaysia and Venezuela and caused the transshipment of U.S.-origin EAR99 items to Iran and Syria without the required U.S. Government authorization. The items exported to non-embargoed destinations were controlled by the U.S. Department of Commerce for reasons of chemical and biological weapons proliferation and required licenses for export to China, Singapore, Malaysia, and Venezuela. This case resulted from an investigation conducted by OEE's Dallas Field Office.



**The Penalty:** On September 29, 2011, Flowserve Corporation and ten of its foreign affiliates agreed to pay civil penalties totaling \$2.5 million. The settlement also required external audits of Flowserve's compliance program. Flowserve also agreed to pay OFAC a civil penalty of \$502,408 for transactions involving Iran, Sudan and Cuba.

**Voluntary Self-Disclosure:** Flowserve voluntarily disclosed these violations, and cooperated fully with the investigation.

### **Buehler Limited**

---

**The Violation:** Between November 2001 and July 2006, Buehler Limited of Lake Bluff, Illinois, a global manufacturer of scientific equipment and supplies for use in materials research and analysis, made 80 exports of a product called "Coolmet," a mixture containing triethanolamine (TEA) that is used as a lubricant with cutting tools, to various destinations including China, Hong Kong, Thailand, India, Brazil and Israel, without the required BIS licenses. Additionally, on one occasion in August 2005, the company's German affiliate re-exported Coolmet from Germany to Iran without the required U.S. Government authorization. TEA is a Schedule 3 chemical precursor classified under ECCN 1C350 and is controlled for chemical/biological, anti-terrorism and chemical weapons reasons. This case resulted from an investigation conducted by OEE's Chicago Field Office.

**The Penalty:** On December 12, 2008, Buehler Limited agreed to pay a \$200,000 civil penalty.

**Voluntary Self-Disclosure:** Buehler Limited voluntarily disclosed the violations and cooperated fully with the investigation.

## Dr. Thomas Butler

**The Violation:** On January 14, 2003, Dr. Thomas Campbell Butler, M.D., a professor at Texas Tech University in Lubbock, Texas, reported to the FBI that thirty vials of a potentially deadly plague bacteria, *Yersinia pestis* (the causative agent of human plague), were missing and presumed stolen from his research lab. The report sparked a



bio-terrorism alert in west Texas, and the President was informed of the incident. An investigation ultimately proved that Dr. Butler had illegally exported *Yersinia pestis* to Tanzania. The bacteria is classified under ECCN 1C351 and cannot be exported to Tanzania without an export license from BIS. On January 15, 2003, Dr. Butler was arrested. Dr. Butler was found guilty of numerous charges at trial, two of which were export control-related: making false, fraudulent and fictitious statements regarding the export to federal agents, and making an unauthorized export to Tanzania. This case resulted from a joint investigation by OEE's Dallas

Field Office, the FBI, IRS, and Department of Transportation.

**The Penalty:** Dr. Butler was convicted of forty-seven counts of a sixty-nine count indictment. He was sentenced to two years in prison on March 10, 2004, and he resigned from Texas Tech. On October 24, 2005, the U.S. Court of Appeals for the Fifth Circuit affirmed his conviction. In the administrative case, on September 1, 2006, Dr. Butler agreed to pay a \$37,400 civil penalty and accept a denial of his export privileges for a period of ten years.



*On the left, biological vectors hidden in a box of baby clothes, on the right, being hand carried on a flight from the United States to Iran. The items were seized as part of an ongoing OEE criminal investigation.*

## *Missile Technology Controls:*

### **Erdal Kuyumcu / Global Metallurgy**

---

**The Violation:** On June 14, 2016, Erdal Kuyumcu, CEO for Global Metallurgy of Queens, New York, pled guilty to violating the IEEPA in connection with the illegal export of a specialized metallic powder designated EAR99 used in aerospace, missile production and nuclear applications to Iran. Kuyumcu and others conspired to obtain more than 1,000 pounds of the metallic powder from a U.S.-based supplier. To hide the true destination of the goods from the supplier, Kuyumcu arranged for the metallic powder to be shipped first to Turkey and then to Iran. Kuyumcu used coded language when discussing the shipment with a Turkey-based co-conspirator, such as referring to Iran as the “neighbor.” This case resulted from a joint investigation conducted by OEE’s New York Field Office and the FBI.

**The Penalty:** On September 7, 2017, Erdal Kuyumcu was sentenced in U.S. District Court for the Eastern District of New York to 57 months in prison, three years of probation, and a \$7,000 fine. On April 9, 2018, BIS issued an order denying Kuyumcu’s export privileges for ten years (until September 7, 2027).

### **Weiss Envirotronics**

---

**The Violation:** Starting on March 27, 2010 through September 11, 2013 Weiss Envirotronics of Grand Rapids, Michigan exported environmental test chambers, classified under ECCN 9B106 and controlled for missile technology reasons and valued at approximately \$3,626,741, to China without the required BIS export licenses. This case resulted from an investigation conducted by OEE’s Chicago Field Office.

**The Penalty:** On June 3, 2016, Weiss Envirotronics agreed to pay a \$575,000 civil penalty, of which \$400,000 was suspended during a two-year probationary period. The agreement also includes a requirement that Weiss Envirotronics conduct two audits, one of which must be conducted by a third party, relating to Weiss Envirotronics’ compliance with U.S. export control laws.

**Voluntary Self-Disclosure:** Weiss Envirotronics voluntarily disclosed these violations, and cooperated fully with the investigation.

### **C.A. Litzler Co., Inc.**

---

**The Violation:** In May 2005, Western Advanced Engineering Company (WAEC) of Orange, California, exported a hot melt prepreg machine for uni-directional tape valued at \$825,000 to Spain without the required export license. The prepreg machine was classified under ECCN 1B001 and was controlled for missile



technology reasons for export to Spain. BIS initially filed a Charging Letter against WAEC. In March 2011, C.A. Litzler Co., Inc. of Cleveland, Ohio, acquired at least a substantial portion of WAEC’s assets, and in June 2013 BIS moved to amend the Charging Letter that was pending before an administrative law judge (ALJ) to add Litzler to the case as a successor in interest to WAEC. In August 2013, the ALJ granted BIS’s motion to add granted BIS’s motion to add Litzler as an additional respondent. This case resulted from an investigation conducted by OEE’s Los Angeles Field Office.

**The Penalty:** On April 24, 2014, C.A. Litzler Co., Inc. agreed to pay a \$45,000 civil penalty. Additionally, on June 12, 2014, WAEC agreed to a three-year suspended denial order.



## Ming Suan Zhang

---

**The Violation:** In 2012, Ming Suan Zhang, a citizen of China, came to the attention of federal authorities after two accomplices attempted to locate large quantities of aerospace-grade carbon fiber via remote Internet contacts. Zhang told an undercover law enforcement agent that he had an urgent need for the specialized carbon fiber in connection with the scheduled test flight of a Chinese fighter plane. Zhang then arranged a meeting in the United States with an undercover agent to take possession of a carbon fiber sample, which was supposed to be shipped to China and analyzed to verify its authenticity. Zhang was placed under arrest after he arrived for the meeting. The scheme was aimed at obtaining thousands of pounds of the high -grade fiber. In August 2013, Zhang pled guilty to violating the IEEPA. This case resulted from a joint investigation conducted by OEE's New York Field Office and ICE.

**The Penalty:** On December 10, 2013, Zhang was sentenced in the U.S. District Court for the Eastern District of New York to 57 months in prison, \$1,000 forfeiture, and a \$100 special assessment. On September 15, 2014, BIS issued an order denying Zhang's export privileges for a period of ten years (until December 10, 2023).

## GrafTech International Holdings Inc.

---

**The Violation:** Between July 2007 and January 2010, GrafTech International Holdings Inc. (GrafTech), of Parma, Ohio, exported twelve shipments of CGW grade graphite to China and India without the required BIS licenses. The high-grade graphite, valued at approximately \$524,000, is classified under ECCN 1C107 and controlled for missile technology reasons. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On October 25, 2013, GrafTech agreed to pay a \$300,000 civil penalty. The agreement also includes an external audit requirement relating to GrafTech's compliance program and the compliance programs of three foreign GrafTech subsidiaries.

**Voluntary Self-Disclosure:** GrafTech voluntarily disclosed the violations and cooperated fully with the investigation.

## Parthasarathy Sudarshan / Mythili Gopal / Cirrus Electronics LLC

---

**The Violation:** Between 2002 and 2006, Parthasarathy Sudarshan, of Simpsonville, South Carolina, president of Cirrus Electronics LLC (Cirrus), with offices in Simpsonville, South Carolina, Singapore, and Bangalore, India, conspired with others, including Mythili Gopal, to illegally export U.S.-origin microprocessors and electronic components for space launch vehicles and ballistic missile programs to the Vikram Sarabhai Space Centre (VSCC) and Bharat Dynamics, Ltd. (BDL), two Indian government entities involved in rocket and missile production, without the required licenses. At the time of the investigation, the commodities were classified under ECCNs 3A001, 3A991, or designated as EAR99. In addition, VSCC and BDL were listed on the BIS Entity List. Sudarshan and others at Cirrus provided the U.S. vendors of electrical components with fraudulent end-use certificates and routed them through the Singapore office to conceal the ultimate destination of the goods. On June 1, 2007, BIS imposed a 180-day Temporary Denial Order (TDO) on Sudarshan, three other Cirrus officials, and the three Cirrus offices (South Carolina, Singapore, and India). Gopal cooperated with the government against her co-conspirator, Sudarshan. This case resulted from a joint investigation conducted by OEE's Washington Field Office and the FBI.

**The Penalty:** On June 16, 2008, Sudarshan was sentenced to 35 months in prison, two years of supervised release, and a \$60,000 criminal fine. Sudarshan will receive credit for time served, which at the time of sentencing was approximately 15 months. The TDO was renewed for an additional 180 days on December 5, 2007. On August 11, 2008, Gopal was sentenced to a \$5,000 fine, four years of probation with the condition of 60 days of home confinement, and 200 hours of community service.



## *National Security Controls:*

### **Zhongxing Telecommunications Equipment Corporation (ZTE) and ZTE Kangxun Telecommunications Equipment**

---

**The Violation** On March 22, 2017, Chinese companies Zhongxing Telecommunications Equipment Corporation and ZTE Kangxun Telecommunications Ltd., known collectively as ZTE, pled guilty in U.S. District Court in the Northern District of Texas in connection with the illegal shipment of telecommunications equipment to Iran and North Korea in violation of the EAR and the ITSR. ZTE conspired to evade the U.S. embargo against Iran in order to obtain contracts with and related sales from Iranian entities, including entities affiliated with the Iranian Government, to supply, build, operate, and/or service large-scale telecommunications networks in Iran, the backbone of which would be U.S.-origin equipment and software. As a result of the conspiracy, ZTE was able to obtain hundreds of millions of dollars in contracts with and sales from such Iranian entities. ZTE also undertook other actions involving 283 shipments of controlled items to North Korea with knowledge that such shipments violated the EAR. Shipped items included routers, microprocessors, and servers controlled under the EAR for national security, encryption, regional security, and/or anti-terrorism reasons. In addition, ZTE engaged in evasive conduct designed to prevent the U.S. Government from detecting its violations. OEE learned that in November 2013, following a meeting of senior managers chaired by its then-CEO, ZTE made plans to resume transshipments to Iran that would continue during the course of the investigation. On March 7, 2016, BIS sanctioned ZTE by adding it to the BIS Entity List, which created a license requirement to export, reexport, or transfer (in-country) to ZTE any items subject to the EAR. During the course of the investigation, ZTE made knowingly false and misleading representations and statements to OEE or other U.S. law enforcement agencies, including that the company had previously stopped shipments to Iran as of March 2012, and was no longer violating U.S. export control laws. ZTE also engaged in an elaborate scheme to prevent disclosure to and affirmatively mislead the U.S. Government, by deleting and concealing documents and information from the outside counsel and forensic accounting firm that ZTE had retained with regard to the investigation. Following the 2017 settlement, ZTE admitted that it had falsely informed the U.S. Government that the company would or had discipline numerous employees responsible for the violations that led to the March 2017 settlement agreement. ZTE instead rewarded that illegal activity with bonuses. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, ICE, and the FBI.

**The Penalty:** On March 22, 2017, ZTE agreed to a combined civil and criminal penalty of \$1.19 billion, the largest fine and forfeiture ever levied by the U.S. Government in an export control case. ZTE agreed to pay a penalty of \$661 million to BIS, with \$300 million suspended during a seven-year probationary period. ZTE also agreed to pay the Department of the Treasury's Office of Foreign Assets Control \$100,871,266 pursuant to a settlement agreement. In addition to these monetary penalties, ZTE agreed to active audit and compliance requirements designed to prevent and detect future violations and a seven-year suspended denial of export privileges. On April 15, 2018, BIS activated the suspended denial order against ZTE in response to the company's admission that it had made false statements to the U.S. Government. On June 8, 2018, BIS and ZTE agreed to a superseding settlement agreement including a civil penalty of \$1.4 billion, of which ZTE paid \$1 billion out-of-pocket and deposited \$400 million into an escrow account in a U.S. bank, where it would remain for ten years unless the company violated U.S. export controls. ZTE also agreed to a ten-year suspended denial order and the retention of a Special Compliance Coordinator, selected by BIS, and paid by ZTE.

### **Peter Zuccarelli / Syed Razvi / American Coating Technologies**

---

**The Violation:** Between approximately June 2015 and March 2016, Peter Zuccarelli and Pakistani naturalized U.S. citizen Syed Razvi agreed to illegally export space-grade radiation hardened integrated circuits (RHICs) to China and Russia. The microchips, classified under ECCN 9A515, are used in satellites and space probes but also have military uses, such as guiding ballistic missiles. In furtherance of the conspiracy, Razvi received purchase orders from customers seeking to purchase RHICs for use in China's and Russia's space programs. Zuccarelli, owner/CEO of American Coating Technologies, in Carrollton, Texas, received these orders from Razvi, as well as payment of

approximately \$1.5 million to purchase the RHICs for the Chinese and Russian customers. Zuccarelli placed orders with U.S. suppliers, and used the money received from Razvi to pay the U.S. suppliers. In communications with the U.S. suppliers, Zuccarelli certified that his company, American Coating Technologies was the end user of the RHICs, knowing that this was false. Zuccarelli received the RHICs he ordered from U.S. suppliers, removed them from their original packaging, repackaged them, falsely declared them as “touch screen parts,” and shipped them out of the U.S. without the required licenses. In an attempt to hide the conspiracy from the U.S. government, he created false paperwork and made false statements. On June 25, 2018 and August 3, 2017, Razvi and Zuccarelli, respectively, pled guilty in U.S. District Court for the Eastern District of Texas. This case resulted from a joint investigation conducted by OEE’s Dallas Field Office, the FBI, ICE, DCIS, and USPIS.

**The Penalty:** On April 22, 2019, Syed Razvi was sentenced to 46 months in prison, three years of supervised release, a \$20,000 criminal fine, and a \$100 special assessment. On January 24, 2018, Peter Zuccarelli was sentenced to 46 months in prison, three years of supervised release, a \$50,000 criminal fine, and a \$100 special assessment.

## Si Chen / Archangel Systems Space

---

**The Violation:** From March 2013 through the end of 2015, Chinese national Si Chen purchased and smuggled sensitive U.S.-origin items classified under ECCN 3A001 to China without obtaining the required BIS licenses. Those items included integrated circuits and other components used in radar and military jamming equipment. Additionally, Chen smuggled communications devices worth more than \$100,000 that are commonly used in space communications applications. Chen falsely under-valued the items on the shipping paperwork to avoid arousing suspicion. Chen received payments for the illegally exported products through an account held at a bank in China by a family member. In addition to participating in the scheme to violate IEEPA, Chen used several aliases and a forged Chinese passport to conceal her smuggling activities. Chen used a Chinese passport bearing her photo and a false name to rent an office in Pomona, California, where she took delivery of the export-controlled items. After receiving the goods, Chen shipped the devices to Hong Kong, and from there the items were transshipped to China. The parcels shipped to Hong Kong bore her false name, along with false product descriptions and monetary values, all done in an effort to avoid attracting law enforcement scrutiny. On July 9, 2018, Chen pled guilty in U.S. District Court for the Central District of California in connection with the procurement scheme; Chen also pled guilty to money laundering and using a forged passport with her photo but a different name that appeared to have been issued. This case resulted from a joint investigation conducted by OEE’s Los Angeles Field Office, ICE and DCIS.

**The Penalty:** On October 1, 2018, Si Chen was sentenced to 46 months in prison, three years of probation, and a \$300 special assessment fee. On August 5, 2019, BIS issued an order denying Si Chen’s export privileges for ten years (until October 10, 2028).

## Bryan Singer

---

**The Violation:** On June 12, 2018, Bryan Singer was found guilty by a jury in the U.S. District Court for the Southern District of Florida in connection with the unlicensed attempted smuggling of electronic devices to Cuba and the making of false statements to federal law enforcement officials. On May 2, 2017, Singer intended to travel from Stock Island, Florida to Havana, Cuba aboard his vessel “La Mala.” Prior to his departure, a U.S. Customs and Border Protection (CBP) agent conducted an outbound inspection of the boat. During the inspection, Singer asserted that he was only bringing to Cuba items observable on the deck and that their value was less than \$2,500. However, the CBP agent discovered a hidden compartment under a bolted down bed in the cabin that contained hundreds of electronic devices valued at over \$30,000. The devices included more than 300 Ubiquiti Nanostation Network devices designed to provide highly encrypted connections between computer networks over long distances. Singer had been previously warned by U.S. Government officials on at least four occasions that a license was required to export items to Cuba. This case resulted from a joint investigation conducted by OEE’s Miami Field Office, ICE, and CBP.

**The Penalty:** On September 27, 2018, Bryan Singer was sentenced in the Southern District of Florida to 78 months in prison, to be followed by supervised release.

## Arc Electronics / Alexander Fishenko / Alexander Posobilov / Shavkat Abdullaev / Anastasia Diatlova

---

**The Violation:** Between 2008 and 2012, Alexander Fishenko, owner of Houston, Texas-based Arc Electronics, and several of its employees obtained advanced microelectronics valued at over \$30 million from manufacturers and suppliers located within the United States and exported those goods to Russia, while carefully evading the government export licensing system. They provided false end-user information in connection with the purchase of the goods, concealed the fact that they were resellers, and falsely classified the goods they exported on export records submitted to the Department of Commerce. The microelectronics shipped to Russia included analog-to-digital converters, static random access memory chips, microcontrollers and microprocessors. These commodities are classified under ECCN 3A001 and are subject to export controls due to their potential use in a wide range of military systems, including radar and surveillance systems, weapons guidance systems, and detonation triggers. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, the FBI, the Naval Criminal Investigative Service, and the Internal Revenue Service.

**The Penalty:** On October 26, 2015, after a month-long trial, Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova were convicted in U.S. District Court for the Eastern District of New York. On February 28, 2017, Posobilov was sentenced to 135 months in prison. In September 2015, Alexander Fishenko pled guilty in connection with the illegal exports. On October 9, 2012, BIS added 165 foreign persons and companies to its Entity List for allegedly engaging in this illegal export scheme.

## Seiler Instruments & Manufacturing Co.

---

**The Violation:** In September 2008, Seiler Instrument & Manufacturing Co., Inc. (Seiler) provided optical instruments to the U.S. Department of Defense pursuant to a government contract. Incorporated into these optical instruments were certain prisms which were purchased by Seiler through an intermediary entity which obtained them from an entity in China where the prisms were manufactured. Seiler and its employees were aware of the origin of these prisms. In submitting the claims for payment on this contract, Seiler, through its employees, stated and represented that the optical instruments were being provided in conformance with the Buy American Act and the applicable Defense Federal Acquisition Regulations. These statements and representations were material to the government making payment to Seiler on the contract. The company admitted in the pretrial diversion agreement that the parts were improperly certified as compliant with the Buy American Act. The pretrial diversion agreement was reached after an investigation into the company's business practices with respect to the full range of import and export regulations governing the procurement of materials used to manufacture defense systems. These provisions place limitations on the export of restricted technical data used in the procurement and manufacturing process to countries such as China. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, DCIS, ICE, and Army CID.

**The Penalty:** On November 21, 2017, Seiler was ordered in U.S. District Court for the Eastern District of Missouri to pay a \$1,500,000 forfeiture.

## Alexy Barysheff / Alexy Krutinin / Dimitri Karpenko

---

**The Violation:** On March 8, 2017, U.S. citizen Alexy Barysheff and Russian nationals Alexy Krutinin and Dimitri Karpenko pled guilty in U.S. District Court for the Eastern District of New York in connection with the unauthorized export of integrated circuits classified under ECCNs 3A001 and 9A515 to Russia. Karpenko and Krutinin were arrested in Colorado in October 2016 and in November 2016 were extradited to the Eastern District of New York. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, ICE and DCIS.

**The Penalty:** On October 19, 2017, Alexy Barysheff was sentenced in U.S. District Court for the Eastern

District of New York to time served and two years of probation. On April 28, 2017, in U.S. District Court for the Eastern District of New York, Alexy Krutinin and Dimitri Karpenko were sentenced to time served and a \$100 special assessment. BIS also issued a Denial of Export privileges for five years for both Krutinin and Karpenko.

### **Millitech, Inc.**

---

**The Violation:** On 18 occasions between 2011 and 2014, Millitech, Inc. of Northampton, Massachusetts engaged in conduct prohibited by the EAR when it exported items subject to the EAR from the U.S. to China



and Russia without the required BIS licenses. Specifically, Millitech Inc. exported active multiplier chains, classified under ECCN 3A001 and controlled for national security and anti-terrorism reasons, valued at approximately \$364,947 to China and Russia. This case resulted from an investigation conducted by OEE's Boston Field Office.

**The Penalty:** On September 25, 2017, Millitech, Inc. agreed to pay a civil penalty of \$230,000.

### **Saeid Charkhian / Caspian Industrial Machinery Supply LLC**

---

**The Violation:** On at least three occasions between 2012 and 2013, Iranian national Saeid Charkhian and Caspian Industrial Machinery Supply LLC, located in the United Arab Emirates (UAE), transferred, forwarded, and /or sold items subject to the EAR and exported from the United States to Iran via the Netherlands and the UAE with knowledge that a violation of the EAR had occurred or was about to occur. The U.S.-origin items included masking wax, lithium batteries, and zirconia crucibles designated EAR99 and valued in total at nearly \$190,000. This case resulted from an investigation conducted by OEE's Boston Field Office.

**The Penalty:** On December 21, 2017, a 12-year denial order was imposed against Charkhian and Caspian Industrial Machinery Supply LLC.

### **Alexander Brazhnikov / ABN Universal**

---

**The Violation:** Alexander Brazhnikov, owner of ABN Universal in Carteret, New Jersey, and his companies were part of a sophisticated procurement network that obtained and smuggled more than \$65 million worth of regulated, sensitive electronic components from American manufacturers and vendors and exported those items to the Federal States Unitary Enterprise Russian Nuclear Center - Academician E.I. Zababkhin All-Russian Scientific Research Institute of Technical Physics, and MIG Electronics, located in Russia. Both companies appear on the BIS Entity List. Brazhnikov was responsible for nearly 2,000 illegal shipments of EAR99 electronics components, many of which wound up in the hands of Russian military and security forces. Brazhnikov also took extensive measure to conceal the true destination of the parts and to conceal the true sources of funds in Russia, as well as the identities of the various Russian defense contracting firms receiving U.S.-origin electronics components. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI and ICE.

**The Penalty:** On June 30, 2016, Alexander Brazhnikov was sentenced in U.S. District Court for the District of New Jersey to 70 months in prison, a \$75,000 criminal fine, a \$65 million forfeiture, forfeiture of his two houses valued at approximately \$500,000 each, and a \$300 special assessment.

## Daofu Zhang / Jian Guanghou Yan / Xianfeng Zuo

---

**The Violation:** Daofu Zhang, Jian Guanghou Yan and Xianfeng Zuo, all Chinese nationals, each operated businesses in China that bought and sold electronic components, including integrated circuits. In 2015, Zuo requested that Yan locate and purchase several advanced integrated circuits which had military applications, including radiation tolerance for uses in space. Yan then asked a U.S. individual to locate the items and sell them to Yan. The U.S. individual explained that the items cannot be shipped outside the United States without an export license, but Yan still wished to make the purchase. When the U.S. individual expressed concern that the desired integrated circuits would have to be stolen from military inventory, Yan proposed to supply the U.S. individual with fake integrated circuits to replace the ones to be stolen from the military. In November 2015, Zhang shipped from China to the U.S. individual, two packages containing counterfeit integrated circuits, each bearing a counterfeit brand label. After further discussions between Yan and the U.S. individual, Yan, Zhang, and Zuo flew together from China to the U.S. in early December 2015 to complete the purchase of the integrated circuits. On December 10, 2015, Yan, Zhang, and Zuo drove to a location in Connecticut, where they planned to meet the U.S. individual, make payment, and take custody of the items. Yan, Zhang, and Zuo were arrested at the meeting location. On April 15, 2016, Zhang pled guilty to charges related to the sale of counterfeit parts intended for the U.S. military in connection with the attempted export of computer chips to China without the required export license. On March 7 and March 16, 2016 respectively, Yan and Zuo pled guilty in connection with the conspiracy. This case resulted from a joint investigation conducted by OEE's Boston Field Office, ICE, DCIS, USAFO, and the FBI.

**The Penalty:** On July 8, 2016, Zhang was sentenced to 15 months in prison. On November 4, 2016, Zuo was sentenced to 15 months in prison. On December 20, 2016, Yan was sentenced to 12 months in prison. In addition, all three defendants' sentences included a \$63,000 forfeiture.

## Unisol International

---

**The Violation:** On five occasions between approximately December 31, 2012, and approximately March 25, 2013, Unisol International sold and/or transferred for export items subject to the EAR with knowledge that a violation of the EAR was occurring, or about to occur, or was intended to occur in connection with the items. Unisol International sold and/or transferred thermal imaging cameras classified under ECCN 6A003, controlled for national security and regional stability reasons, and valued at \$67,080, for export from the United States to Ecuador, Venezuela, and Mexico without the BIS licenses required for these exports. Unisol International knew or had reason to know that it was about to violate the EAR because in December 2012, a U.S. company notified Unisol International in writing, including specifically Unisol International's chief executive officer, that the items were controlled for export purposes and required a BIS license to export. This company also discussed the applicable ECCN, referred Unisol International to the EAR and BIS's website, and offered to answer any questions Unisol International might have. Nonetheless, Unisol International subsequently completed the sale and/or transfer of the items for export, and exported them to Ecuador, Venezuela and Mexico without seeking BIS licenses. This case resulted from an investigation conducted by OEE's Miami Field Office.

**The Penalty:** On May 24, 2016, Unisol International agreed to pay \$250,000 in civil penalties, of which \$100,000 is suspended during a two-year probationary period.

## Mark Henry

---

**The Violation:** On July 2, 2014, Mark Henry was found guilty by a jury in U.S. District Court for the Eastern District of New York of conspiracy to violate the Arms Export Control Act. In May 2012, Henry attempted to export two microwave amplifiers classified under ECCN 3A001 and valued at over \$70,000 to China without the required license. Special Agents from the New York Field Office performed a controlled delivery, intercepted the shipment, and executed a search warrant on Henry's home and the boxes containing the amplifiers. Henry was subsequently indicted and arrested. During the trial, Special Agents testified under direct and cross examination, and over 1,000 exhibits were introduced as evidence. This case resulted from an investigation conducted by OEE's New York Field Office.



**The Penalty:** On November 19, 2015, Mark Henry was sentenced in U.S. District Court for the Eastern District of New York to 78 months in prison, three years of probation, and a \$200 special assessment. The District Court Judge added a two-point enhancement for perjury, and three points were added because Henry had a criminal history. On September 28, 2017, a Final Order was issued denying Henry's export privileges for a period of ten years, as well as those of related party Dahua Electronics Corporation, located in Flushing, New York.

## **Streit USA Armoring LLC / Streit Middle East / Streit Group FZE / Guerman Gouterov / Eric Carlson**

---

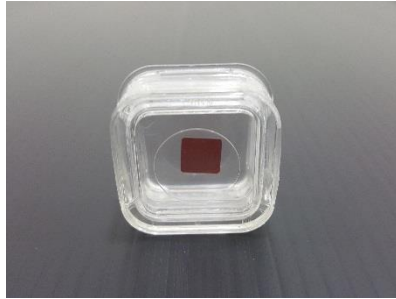
**The Violation:** Between March 2008 and November 2009, Streit USA Armoring LLC ("Streit USA") of North Charleston, South Carolina, Streit Middle East of Dubai, United Arab Emirates ("UAE"), and Streit Group FZE of the Ras-Al Khaimah Free Trade Zone, UAE (collectively, "the Streit Group") violated the EAR by making or causing unauthorized resales, transfers, exports or reexports of U.S.-origin armored vehicles, including in violation of license conditions, and by making false statements in connection with license applications and failing to update license applications as material or substantive facts changed. The items were classified under ECCN 9A018, controlled on national security grounds, valued in total at some \$3.1 million, and exported or reexported to Afghanistan, Iraq, Nigeria, the Philippines, Singapore, and Venezuela. The Streit Group's owner/CEO and a Streit USA corporate officer caused/aided/abetted some of the violations through their actions and/or inaction. Streit USA possessed a BIS license to export such armored vehicles to the UAE, but the license required Streit USA to inform the consignee of all license conditions, including that no resale, transfer, or reexport of the items was permitted without prior authorization by the U.S. Government. Streit USA failed to inform Streit Middle East, the consignee, of the license condition prohibitions until 19 months later, even though aware that Streit Middle East and Streit Group FZE were engaging in unlicensed resales, transfers, and reexports. Despite this knowledge, Streit USA exported the items to Streit Middle East in the UAE. Streit Middle East and Streit Group FZE continued to engage in unlicensed transactions even after learning of the license requirement and being warned of the penalties for noncompliance. Guerman Gouterov, the chairman, CEO, and sole or majority owner of the Streit Group entities, also had personal knowledge of these warnings and related transactions, but failed to prevent the transactions and violations from continuing. When Streit USA finally did seek a BIS license for Streit Middle East to reexport some of the vehicles to Iraq and the Philippines, it made a false statement and/or failed to update the applications despite knowing the vehicles would actually be reexported by Streit Group FZE and learning that Streit Group FZE intended to proceed with the Iraq reexport without the required license. Streit USA also has applied for a license to export armored vehicles to Venezuela, but just three weeks later, while the application remained pending, transferred the vehicles to a Canadian affiliate despite knowing the items would immediately be transshipped to Venezuela without the required license. When BIS forwarded questions about the application the following month, as part of the interagency license review process, Streit USA falsely told BIS that the sale had been lost. Streit USA then-Vice President (and subsequently President) Eric Carlson was directly involved in this false statement scheme, as was Streit Group FZE. These cases resulted from a joint investigation conducted by OEE's Washington Field Office and ICE.

**The Penalty:** On September 1, 2015, BIS imposed civil penalties totaling \$3.5 million against these respondents pursuant to settlement agreements with them, including \$1.6 million against Streit USA (with \$850,000 suspended), \$1.6 million jointly and severally against Streit Middle East and Streit Group FZE (with \$850,000 suspended), \$250,000 against Gouterov, and \$50,000 against Carlson. Each of the companies was also required to complete two audits of their compliance programs. All of the respondents were subject to three-year suspended denial orders. The suspensions of portions of the Streit USA and Streit Middle East/Streit Group FZE penalties were subject to a three-year probationary period and related compliance conditions. On April 14, 2017, BIS issued an Order accelerating the two remaining \$170,000 installment payments due from Streit USA after the company failed to timely make one of its installment payments as required under the settlement agreement.

## ZhENCHUN “Ted” Huang

---

**The Violation:** ZhENCHUN Huang, also known as Ted Huang, a Chinese national and naturalized U.S. citizen, pled guilty in July 2014 in connection with a scheme to obtain U.S.-origin commodities, which are subject to



the EAR, for export to China by means of false and fraudulent representations. When Huang became aware of the investigation, he absconded from the United States to China and was a fugitive until his arrest in London in December 2013. The items, cadmium zinc telluride and mercury cadmium telluride wafers, were classified under ECCN 3B001 and were controlled for national security reasons. This case resulted from a joint investigation conducted by OEE’s Washington Field Office, the FBI, and the National Aeronautics and Space Administration (NASA) Office of Inspector General.

**The Penalty:** On October 20, 2014, Huang was sentenced to 15 months in prison, three years of probation, and a \$200 special assessment.

## Zhen Zhou Wu / Yufeng Wei / Bo Li / Chitron Electronics, Inc.

---

**The Violation:** On May 17, 2010, Zhen Zhou Wu, aka Alex Wu, Yufeng Wei aka Annie Wei, and Chitron Electronics, Inc. (Chitron-US), located in Waltham, Massachusetts, were convicted of unlawfully exporting defense articles and goods controlled by BIS for national security reasons through Hong Kong to China between 2004 and 2007 in violation of U.S. export control laws. Bo Li, aka Eric Lee, manager of Chitron-US in 2007, Wu and Wei were convicted of filing false shipping documents with the U.S. Department of Commerce in connection with these shipments. In addition, Wei was convicted of immigration fraud. The exported equipment is classified as ECCN 3A001 and is used in electronic warfare, military radar, fire controlling, military guidance and control equipment, and satellite communications, including global positioning systems. This case resulted from a joint investigation conducted by OEE’s Boston Field Office, the FBI, ICE and DCIS.

**The Penalty:** On January 28, 2011, Chitron-US was sentenced to a \$15.5 million fine, a special assessment of \$10,400, and a shared forfeiture with Wu and Wei of \$65,881. On January 28, 2011, Annie Wei was sentenced to 36 months in prison and the shared forfeiture. On January 26, 2011, Wu was sentenced to 97 months in prison, 24 months of supervised release, and a criminal fine of \$15,000, a \$1,700 special assessment, and the shared forfeiture. On February 9, 2011, Shenzhen Chitron Electronics Company Limited (Chitron -Shenzhen) was ordered to pay \$1,925,000 for failing to appear for 77 days in court proceedings related to its involvement in the exports. On July 22, 2010, Eric Lee was sentenced to 11 months in prison (time served), three years of supervised release, a \$1,000 fine, and a \$100 special assessment. On June 4, 2012, BIS issued denial orders for 10-years against Wei, Wu, Chitron-Shenzhen, and its two subsidiaries, Chitron-US in Massachusetts and Chitron (HK) Electronics Company Limited in Hong Kong. On March 19, 2013, the U.S. Court of Appeals for the First Circuit in Boston, Massachusetts upheld Wu and Wei’s convictions on all IEEPA counts, one count of conspiracy, and Shipper’s Export Declaration (SED) violations. On September 10, 2013, a re-sentencing hearing for Wu was held, at which he was sentenced to 84 months in prison, a \$15,000 fine, and deportation back to China upon release from prison. On April 30, 2014, a re-sentencing hearing for Wei was held, at which she was sentenced to 23 months in prison, two years of supervised release, and deportation back to China upon release from prison. Chitron-US, Annie Wei and Alex Wu appear on the Department of State’s Debarred List.

## Timothy Gormley / Amplifier Research Corporation

---

**The Violation:** Timothy Gormley was an employee of Amplifier Research Corporation in Souderton, Pennsylvania. Many of this company’s products are classified as ECCNs 3A001 and EAR99 and are controlled for national security reasons with applications in military systems, requiring a license for export to most destinations outside Europe. While working for Amplifier Research Corporation, Gormley altered

invoices and shipping documents to conceal the correct classification of the amplifiers so they would be shipped without the required licenses, listed false license numbers on the export paperwork, and lied to fellow employees about the status and existence of export licenses. Gormley's actions resulted in at least 50 unlicensed exports of national security items to such destinations as China, India, Hong Kong Taiwan, Thailand, Russia, and Mexico. In admitting to the conduct, he explained that he was "too busy" to obtain the licenses. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On January 17, 2013, Gormley was sentenced to 42 months in prison, five years of supervised release, a \$1,000 criminal fine and a \$500 assessment. On December 27, 2013, Amplifier Research agreed to a fully suspended civil penalty of \$500,000 provided the company does not commit any export violations for two years. Additionally, Amplifier Research is required to conduct external audits of their compliance programs and submit the results to BIS.

**Voluntary Self-Disclosure:** Amplifier Research voluntarily disclosed the violations and cooperated fully with the investigation.

## ***Crime Controls:***

### **Patrick Germain**

---

**The Violation:** On October 9, 2018, Patrick Germain pled guilty in U.S. District Court for the Northern District of Illinois in connection with the illegal export of firearms to Haiti. In June 2016, Germain purchased 26 firearms, five shotguns classified under ECCN 0A984, and ammunition from dealers in Illinois. Germain also purchased three vehicles, including the cargo van that he would later use to transport the concealed firearms and ammunition. He then hired an Illinois company to deliver the three vehicles to Miami, where he arranged for a Florida shipping company to transport the vehicles to Haiti. Germain devised a scheme to hide some of the items inside a hollowed-out wooden container constructed of plywood in a van he arranged to export through the Port of Miami to Haiti. When asked by the Illinois company why the cargo van appeared to be overweight, Germain represented to the driver that the added weight was due to furniture in the back seat. The van was detained and the firearms located. Germain was arrested in December of 2016 when he returned to the United States from Haiti. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, ICE, and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

**The Penalty:** On May 16, 2019, Patrick Germain was sentenced in U.S. District Court for the Northern District of Illinois to time served in prison (23 days), two years of supervised release, and a \$100 special assessment.

### **Rasheed Al Jjakli / Palmyra Corporation**

---

**The Violation:** From June through July of 2012, Syrian-born naturalized U.S. citizen Rasheed Al Jjakli and a co-conspirator purchased tactical gear, including day vision and night vision rifle scopes classified under ECCN 0A987, laser boresighters, flashlights, radios and other items designated EAR99, for intended end use in Syria. On July 17, 2012, Al Jjakli traveled with the tactical gear from Los Angeles to Istanbul with the intent that it would be provided to Syrian rebels training in Turkey and fighting in Syria. Al Jjakli provided some of the tactical gear, specifically the laser boresighters, to a second co-conspirator, who Al Jjakli learned was a member of the militant group Ahrar Al-Sham. Al Jjakli also provided the goods to other armed Syrian insurgent groups in Syria and Turkey. Additionally, in August and September 2012, Al Jjakli directed co-conspirators to withdraw thousands of dollars from Palmyra Corporation, where Al Jjakli was the chief executive officer, to pay for tactical gear that would be provided to Syrian rebels. In his plea agreement, Al Jjakli specifically admitted directing that \$17,000 from Palmyra be used to purchase tactical gear intended for Syrian rebels. On August 13, 2018, Al Jjakli pled guilty in connection with a conspiracy to illegally export tactical gear to Syria. During Al Jjakli's sentencing hearing, the Judge agreed with prosecutors that the goods Al Jjakli took to Syria were "instruments of death." This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, the FBI, ICE, and the IRS.

**The Penalty:** On December 20, 2018, Rasheed Al Jijakli was sentenced to 46 months in prison, two years of supervised release, a \$5,000 criminal fine, and a \$100 special assessment.

### **Kenneth Chait / Tubeman.com/Advantage Tube Services, Inc.**

---

**The Violation:** In October 2012, U.S. citizen Kenneth Chait, owner/operator of Tubeman.com/Advantage Tube Services, Inc., located in Lake Worth, Florida, communicated to an undercover OEE Special Agent that he was willing to export to Pakistan two ceramic metal triggered spark gaps (also known as nuclear trigger spark gaps), without the required BIS export license. The spark gaps were listed on the Commerce Control List, controlled for nuclear proliferation reasons, and therefore required a license for export to Pakistan. ICE Special Agents then conducted undercover operations by speaking with Chait regarding obtaining a ceramic metal triggered spark gap classified under ECCN 3A228 for export to Pakistan. Chait was arrested in March 2014 during execution of a search warrant, and in April 2015, he pled guilty in U.S. District Court for the Middle District of Georgia to violations of the International Emergency Economic Powers Act and the EAR in connection with the attempted export of nuclear trigger spark gaps to Pakistan without a license. This case resulted from a joint investigation conducted by OEE's Miami Field Office and ICE.



**The Penalty:** On November 13, 2018, Kenneth Chait was sentenced to 12 months and one day in prison, two years of supervised release, and a \$100 special assessment. As part of the plea agreement, Chait agreed to forfeit \$7,465 to the U.S. Government, which represents the proceeds traceable to the undercover transactions in which he participated.

### **Dmytro Medvedyev**

---

**The Violation:** On November 30, 2016, Ukrainian national Dmytro Medvedyev pled guilty in U.S. District Court for the District of Delaware in connection with identity theft crimes. Medvedyev utilized stolen identities to purchase rifle scopes classified under ECCN 0A987 and smuggle them to Ukraine. In October 2015, OEE Special Agents interdicted 10 of these rifle scopes at freight forwarder located in Delaware. This case resulted from a joint investigation conducted by OEE's Washington Field Office, the FBI and ICE.

**The Penalty:** On August 30, 2017, Dmytro Medvedyev was sentenced in U.S. District Court for the District of Delaware to 36 months in prison and restitution in the amount of \$14,200, one year of probation, and a \$300 special assessment.

### **Shehzad John**

---

**The Violation:** On January 11, 2016, Shehzad John pled guilty in connection with the illegal export of optical rifle sights classified under ECCN 0A987 and controlled for crime control reasons to Pakistan. In September 2013, John attempted to export assault rifles, 9mm pistols, scopes, and laser sights, bought by straw purchasers on his behalf, to Pakistan aboard a commercial airliner without the required export licenses. John was arrested at JFK International Airport in November 2014 and indicted in April 2015. This case resulted from a joint investigation conducted by OEE's New York Field Office, ICE, and ATF.

**The Penalty:** On August 1, 2016, Shehzad John was sentenced in U.S. District Court for the Southern District of New York to 71 months in prison, three years of supervised release, a \$10,000 criminal fine, and a \$100 special assessment. On September 28, 2017, a Final Order was issued denying John's export privileges for a period of ten years.



*OEE Special Agents executing a search warrant.*

## Kan Chen

---

**The Violation:** On March 2, 2016, Kan Chen of Ningbo, China entered a guilty plea in U.S. District Court for the District of Delaware in connection with the illegal export of over 180 export-controlled items valued collectively at over \$275,000 from the United States to China. The items exported primarily included night vision and thermal imaging rifle scopes, as well as rifle scopes with combat applications. Most of these items were classified under ECCN 0A987 and controlled for Crime Control reasons. Given the sensitivity surrounding these military-grade items, Chen devised a scheme to smuggle these items through Delaware and outside the United States. He purchased the devices via the internet and telephone and had them mailed to several reshipping services in New Castle, Delaware. These Delaware-based service companies provide an American shipping address for customers located in China, accept packages for their customers, and then re-ship them to China. In order to further conceal his illegal activity, Chen arranged for the re-shippers to send the devices to several intermediary individuals, who in turn forwarded the devices to Chen in China. Chen then sent the devices onwards to his customers. During the course of this conduct, Chen made numerous false statements in order to knowingly and willfully evade the export control laws of the United States. These false statements included undervaluing the shipments, unlawfully avoiding the filing of export information with the U.S. Government, indicating that he was a natural-born U.S. citizen, and providing the address of the reshipping service as his own. Chen was arrested by federal agents on the Northern Mariana Island of Saipan following an eight-month long investigation into his illegal conduct. This case resulted from a joint investigation with OEE's Washington Field Office and ICE.

**The Penalty:** On June 29, 2016, Chen was sentenced to 30 months in prison, three years of supervised release, and a \$300 special assessment.

## Hassan Salame

---

**The Violation:** On April 15, 2015, Hassan Jamil Salame pled guilty in U.S. District Court for the District of South Carolina to charges related to the attempted smuggling of shotguns and other firearms and ammunition classified under ECCN 0A984 from the United States to Lebanon. Salame attempted to export the items to Lebanon without the required export licenses and knowingly failed to declare the items on SEDs. This case resulted from a joint investigation with OEE's Washington Field Office, ICE, ATF, and CBP.

**The Penalty:** On November 3, 2015, Salame was sentenced to 45 months in prison, 36 months of probation, and a \$300 special assessment. Additionally, Salame agreed to a 10-year denial of export privileges.



## **B&H Foto & Electronics Corp.**

---

**The Violation:** Between 2009 and 2012, B&H Foto & Electronics Corp. of New York, New York, made 50 exports of optical sighting devices classified as ECCN 0A987 to a variety of countries, including Russia, Kazakhstan, Hong Kong, Saudi Arabia and South Africa without the required BIS licenses. The optical sighting devices, valued at \$23,000, were controlled for crime control reasons. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On January 8, 2015, B&H Foto & Electronics Corp. agreed to pay a \$275,000 civil penalty.

## **Mike Cabatingan / Romulo Reclusado**

---

**The Violation:** On May 8, 2013, Romulo Reclusado pled guilty to conspiracy for his role in the export of controlled holographic rifle sights to the Philippines without first obtaining a BIS license in violation of the IEEPA and International Traffic in Arms Regulations. On February 7, 2011, Mike Cabatingan, a co-defendant of Reclusado, pled guilty in to conspiracy to violate the Arms Export Control Act and the IEEPA. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office, ICE and DCIS.

**The Penalty:** On March 9, 2015, Mike Cabatingan was sentenced U.S. District Court for the Central District of California to 12 months and one day in prison, a \$7,500 criminal fine, and two years of supervised release. On November 13, 2013, Romulo Reclusado was sentenced in U.S. District Court for the Central District of California to 60 months in prison, three years of supervised release, and a \$7,500 criminal fine.

## **Lev Steinberg**

---

**The Violation:** On September 16, 2009, Lev Steinberg, a resident of Brooklyn, New York, pled guilty to violating the IEEPA and the Foreign Corrupt Practices Act. Steinberg was arrested in March 2009 for exporting rifle scopes classified under ECCN 0A987 and controlled for crime control reasons to Russia without the required license from BIS. This case resulted from a joint investigation conducted by OEE's New York Field Office, ICE, and DCIS.

**The Penalty:** On February 25, 2014, Lev Steinberg was sentenced to one year of probation, a \$4,000 criminal fine, and a \$200 assessment. On November 20, 2014, a Final Order was issued denying Steinberg's export privileges for a period of two years.

## **Vitali Tsishuk / Volha Dubouskaya / Aliaksandr Stashynski / Yahor Osin / Aliaksandr Belski / Ernest Chornoletskyy**

---

**The Violation:** In August 2011, Aliaksandr Stashynski, Yahor Osin, Aliaksandr Belski, Vitali Tsishuk, and Volha Dubouskaya, Belarussian citizens living in Pennsylvania, as well as Ernest Chornoletskyy, a Ukrainian citizen living in Pennsylvania, were charged with criminal conspiracy to export defense articles without a State Department license and conspiracy to violate IEEPA. Osin, Belski, and Tsishuk were further charged with conspiracy to launder monetary instruments. The defendants conspired to illegally export to Belarus numerous defense articles, including Thermal Imaging Scopes, Mini Thermal Monoculars, and Thermal-Eye Renegade-320s, without obtaining a license from the Department of State. During this period, the defendants also conspired to illegally export Commerce-controlled items to Belarus, including L-3 x 200xp Handheld Imaging Cameras classified as ECCN 0A987 controlled for crime control reasons, without a BIS license. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI and ICE.

**The Penalty:** In February 2013, Tsishuk was sentenced to 24 months in prison for his role in the conspiracy. Dubouskaya and Stashynski were each sentenced to six months in prison, three-year supervised release, and a \$3,000 criminal fine. On July 18, 2013, Belski was sentenced to 57 months in prison, two years of supervised release, a \$3,000 criminal fine, and a \$300 special assessment. In August 2013, Chornoletskyy, was convicted of conspiracy and violating IEEPA. He was sentenced to 15 months imprisonment, three years of supervised release, a \$3,000 criminal fine, and \$200 special assessment. BIS imposed ten-year Denial Orders against Dubouskaya, Stashynski, and Chornoletskyy.

### **Mark Komoroski / Sergey Korznikov / D&R Sports Center**

---

**The Violation:** On August 4, 2009, Mark Komoroski, owner of D&R Sports Center, of Nanticoke, Pennsylvania, pled guilty to one count of conspiracy to violate IEEPA and the Arms Export Control Act, filing improper records maintained by a firearms dealer, mail fraud, smuggling, and money laundering. The charges related to the export of rifle scopes, classified as ECCN 0A987, to Russia without the required licenses from BIS and the Department of State. On December 28, 2010, co-conspirator Sergey Korznikov pled guilty in U.S. District Court in the Middle District of Pennsylvania to one count of conspiracy related to his involvement in smuggling items from the United States. This case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, and DCIS.



**The Penalty:** On July 21, 2011, Korznikov was sentenced to six months in prison, two years of supervised release and a \$100 special assessment. On July 29, 2010, Komoroski was sentenced to 32 months in prison, a \$10,000 criminal fine, two years of supervised release, and a \$100 special assessment.



*Rifles, pistols, magazines and ammunition seized by OEE Special Agents as part of an ongoing criminal investigation.*

# Chapter 3 – Freight Forwarders

## Introduction

Primary responsibility for compliance with the EAR generally falls on the “principal parties in interest” in a transaction, who are usually the U.S. seller and the foreign buyer. However, freight forwarders or other agents acting on behalf of the principal parties are also responsible for their actions, including the representations they make by signing an export declaration or other export control document.

To help avoid liability in an export transaction, agents and exporters must decide whether any aspect of the transaction raises red flags, inquire about those red flags, and ensure that suspicious circumstances are not ignored. Both the agent and the principal party are responsible for the accuracy of each entry made on an export document. Good faith reliance on information provided by the exporter may excuse an agent’s actions in some cases, but the careless use of pre-printed “No License Required” forms or unsupported entries can get an agent into trouble.

## Criminal and Administrative Case Examples

### Eric Baird / Access USA Shipping, LLC

**The Violation:** On December 12, 2018, Eric Baird, the former owner and Chief Executive Officer (CEO) of Access, a Florida-based package consolidation and shipping service, pled guilty in U.S. District Court for the Middle District of Florida to one count of felony smuggling and admitted to 166 administrative violations of U.S. export control laws as part of a global settlement with the U.S. Department of Justice and BIS. Baird admitted to violations of the EAR committed from August 1, 2011, through January 7, 2013, during his tenure as CEO of Access USA Shipping, LLC dba MyUS.com (Access USA). Baird founded Access USA and developed its business model, which provided foreign customers with a U.S. address that they used to acquire U.S.-origin items for export without alerting U.S. merchants of the items’ intended destinations. Under Baird’s direction, Access USA developed practices and policies which facilitated concealment from U.S. merchants. Access USA would regularly change the values and descriptions of items on export documentation even where it knew the accurate value and nature of the items. Among the altered descriptions were some for controlled items listed on the Commerce Control List. For example, laser sights for firearms were described as “tools and hardware,” and rifle scopes were described as “sporting goods” or “tools, hand tools.” The activities that Baird knowingly authorized and/or participated in resulted in unlicensed exports of controlled items to various countries, as well as repeated false statements on AES filings. In doing so he caused, or permitted, the filing of false or misleading SED and AES filings. Baird also failed to make required SED/AES filings and also caused, aided or abetted the export of items subject to the EAR without the required export licenses. As early as September 2011, Baird was made aware that undervaluing violated U.S. export laws, including the EAR. In fact, Baird received e-mails on this subject from his Chief Technology Officer, who stated, “I know we are WILLINGLY AND INTENTIONALLY breaking the law” (emphasis in original). In the same email chain, Baird suggested that Access USA could falsely reduce the value of items by 25% on export control documentation submitted to the U.S. government and if “warned by [the U.S.] government,” then the company “can stop ASAP.” Additionally, Baird established and/or authorized Access USA’s “personal shopper” program. As part of this program, Access USA employees purchased items for foreign customers from a shopping list while falsely presenting themselves to U.S. merchants as the domestic end users of the items. This case resulted from a joint investigation conducted by OEE’s Miami Field Office and ICE.

**The Penalty:** On January 30, 2019, Eric Baird was sentenced to 24 months of probation and a \$100 special assessment. Baird also agreed to a five-year denial of export privileges and a \$17 million fine with \$7 million suspended. Access USA also agreed to an administrative fine of \$27 million with \$17 million suspended.

## Mohawk Global Logistics Corp. / Multiwire Laboratories

---

**The Violation:** In 2014 and 2015, Multiwire Laboratories (Multiwire) of Ithaca, New York, and Mohawk Global Logistics Corp. (Mohawk) of North Syracuse, New York, each violated the EAR when Multiwire, aided and abetted by Mohawk, twice exported camera detectors and accessories designated EAR99 and valued at \$177,156 to the University of Electronic Science and Technology of China (UESTC) in China without the required BIS license. UESTC was listed on the BIS Entity List, and a BIS license was required to export any items subject to the EAR to that entity. Mohawk acted as Multiwire's freight forwarder and Mohawk used screening software in connection with the 2014 transaction, but assertedly did not enter UESTC's full, unabbreviated name (which was known to Mohawk) into the software, which as a result did not "flag" the transaction. Mohawk proceeded with the 2014 transaction and prepared and filed EEI that incorrectly indicated the export was "NLR." In August 2015, Multiwire (again with the assistance of Mohawk) also exported the same items to UESTC, which had been returned to Multiwire for warranty repair. Mohawk also violated the EAR in August 2012, when it aided and abetted the export of a liquid nitrogen plant designated EAR99 and valued at \$33,587 to the All-Russian Scientific Research Institute of Experimental Physics (VNIIEF-VNIEEF), aka Russian Federal Nuclear Center-VNIIEF (RFNC-VNIEEF). VNIEEF and its RFNC-VNIEEF alias were at all relevant times listed on the BIS Entity List. Mohawk was aware of the BIS Entity List and maintained a screening program to detect and prevent shipments to restricted parties. Mohawk compared the name of the ultimate consignee to entries on the BIS Entity List using their screening software, which correctly identified VNIEEF as being listed on the BIS Entity List, and "flagged" the shipment. However, as Mohawk acknowledged to BIS, an export supervisor erroneously overrode or ignored this red flag and Mohawk proceeded without further inquiry or due diligence to forward the items for export. Mohawk prepared and filed EEI with the U.S. Government on or about that date indicating that the shipment was "NLR." The exporter in this transaction was Cryomech, Inc., of Syracuse, New York, and previously agreed to a settlement with BIS on June 9, 2017 for its role in the unlicensed export. This case resulted from an investigation conducted by OEE's New York Field Office.



**The Penalty:** On January 16, 2019, Multiwire was assessed a civil penalty of \$80,000. On August 10, 2018, Mohawk was assessed a civil penalty of \$155,000, \$20,000 of which was suspended during the one-year probationary period and thereafter waived, provided no violations are committed during the probationary period. Cryomech, Inc., was previously assessed a civil penalty of \$28,000 and ordered to complete an external audit of its export compliance program.

## Gennadiy Boyko / SHOPOZZ, Inc.

---

**The Violation:** On December 6, 2017, Gennadiy Boyko pled guilty in U.S. District Court for the Northern District of Georgia in connection with conspiring to violate the IEEPA and the Arms Export Control Act. Boyko is the owner of SHOPOZZ, Inc., a mail consolidation and forwarding business located in Alpharetta, Georgia that provides a virtual U.S. address for individuals located in Russia and Ukraine. Boyko and his co-conspirators utilized his business to illegally export EAR-controlled rifle optics classified under ECCN 0A987 as well as ITAR-controlled weapons parts to Russian and Ukraine. The items were ordered from U.S. online



vendors and then shipped to SHOPOZZ or Boyko's home, repacked with other innocuous items and then shipped out of the country. This case resulted from a joint investigation conducted by OEE's Atlanta Resident Office, the FBI, DCIS, and CBP.

**The Penalty:** On November 28, 2018, Gennadiy Boyko was sentenced to 18 months in prison, one year of supervised release, 100 hours of community service, and a \$100 special assessment.

## Federal Express

---

**The Violation:** On 53 occasions between 2011 and 2012, Federal Express (FedEx), located in Memphis, Tennessee, facilitated the export of civil aircraft parts and equipment used for electronic microscope manufacturing classified under ECCN 9A991 or 7A994, or designated EAR99, and valued at approximately \$58,091 from the United States to Aerotechnic France (Aerotechnic), or to the Pakistan Institute for Nuclear Science and Technology (PINSTECH) in Pakistan, without the required BIS licenses. Aerotechnic was added to the BIS Entity List in June 2011 "based on evidence that [it had] engaged in actions that could enhance the military capability of Iran, a country designated by the U.S. Secretary of State as having repeatedly provided support for acts of international terrorism...[and] because [its] overall conduct pose(d) a risk of ongoing EAR violations." PINSTECH is a subordinate entity of the Pakistan Atomic Energy Commission, and has been on the BIS Entity List since November 1988, when it was added to the BIS Entity List along with a number of other Pakistani government (parastatal and private) entities involved in nuclear or missile activities shortly after Pakistan detonated a nuclear device. This case resulted from an investigation conducted by OEE's Miami Field Office.

**The Penalty:** On April 24, 2018 FedEx agreed to pay a \$500,000 civil penalty.



*OEE Special Agents conducting inspections with U.S. Customs and Border Protection Officers.*

## Pilot Air Freight LLC aka Pilot Air Freight Corp.

---

**The Violation:** During 2015, Pilot Air Freight LLC of Lima, Pennsylvania, violated the EAR by facilitating the attempted unlicensed export of an ultrasonic mill cutting machine classified under ECCN 2B991 and controlled for anti-terrorism reasons, and related electrical equipment designated EAR99, to IKAN Engineering Services (IKAN) in Pakistan. IKAN was added to the BIS Entity List in September 2014, along with several other Pakistani entities that had worked with Pakistan's Advanced Engineering Research



Organization (A ERO) to procure sensitive U.S.-origin technology in support of Pakistan's missile and strategic unmanned aerial vehicle (UAV) programs. The company arranged for the transport of the items by rail to the intended port of export in Long Beach, California, and prepared and submitted shipping documentation, including Electronic Export Information (EEI) filed with the U.S. Government. The EEI indicated, erroneously, that no license was required for export of the items to IKAN. Improperly configured screening software was responsible for the transaction not being flagged for review. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On November 21, 2017, Pilot Air Freight LLC agreed to pay a \$175,000 civil penalty, \$75,000 of which was suspended provided no further violations occur during the probationary period. The company was also ordered to complete two external audit of its export controls compliance program, to be conducted by an unaffiliated third-party consultant.

### **Asim Fareed / Compass Logistics International**

---

**The Violation:** On June 14, 2016, Asim Fareed, a U.S. citizen and Vice President of Compass Logistics International in Somerset, New Jersey, surrendered for arrest and pled guilty in U.S. District Court for the Middle District of Pennsylvania in connection with a conspiracy to make false statements related to the export of U.S.-origin EAR99 commodities to Iran. Fareed operated Compass Logistics, an export business, and agreed to ship items purchased by customers in Iran and to provide false documentation to the U.S. Department of Commerce for export purposes. Fareed prepared invoices which included false information as to the identity and geographic location of the purchasers of the goods. The items were then to be shipped from the United States to the United Arab Emirates, and then transshipped to Iran. This case resulted from a joint investigation conducted by OEE's New York Field Office and ICE. In the related administrative action, BIS charged one count of conspiracy to export \$50,000 in items subject the Regulations from the United States to Iran, via the United Arab Emirates.

**The Penalty:** On September 12, 2016, Fareed was sentenced to two years of probation, a \$1,000 criminal fine, and a \$100 special assessment. On December 19, 2018, BIS issued a Final Order subjecting Fareed to a three-year suspended denial of export privileges and requiring him to submit two annual reports of his export and reexport activities.

### **Fulfill Your Packages**

---

**The Violation:** Fulfill Your Packages (FYP) of Gresham, Oregon, allowed its foreign customers in China to use its U.S. domestic address for the purchase and delivery of items from U.S. companies that FYP later repackaged and/or relabeled for export to China. In about June 2014, FYP engaged in a transaction or took other actions with intent to evade the EAR in connection with the intended export of a FLIR thermal imaging camera classified as ECCN 6A003 and controlled for national security and regional stability reasons. Specifically, a FYP customer purchased the camera from a U.S. distributor located in Florida for delivery to FYP's offices in Oregon and for ultimate export to China. The FYP customer provided FYP's address as his own and did not disclose to the U.S. distributor that the thermal imaging camera was to be exported to China. The shipment from the distributor to FYP included an invoice that warned that the product was export-controlled and that was a violation of U.S. law to export the product to certain countries without the required export license. In addition, a label affixed to the item noted that the item was subject to U.S. Department of Commerce export control regulations and must not be exported outside the United States or Canada without a U.S. export license. In preparing to export the thermal imaging camera to China, FYP prepared a U.S. Postal Service shipping label falsely describing the item as "metal parts" valued at \$255, even though FYP's order system described the items as an infrared webcam/surveillance camera installation kit, and even though the distributor's invoice described the items as a thermal imaging camera valued at \$2,617. This case resulted from a joint investigation conducted by OEE's San Jose Field Office and Portland Resident Office, the FBI and ICE.

**The Penalty:** On June 17, 2016, FYP agreed to pay a \$250,000 civil penalty with \$190,000 suspended provided no violations occur during a two-year probationary period.

## General Logistics International

---

**The Violation:** On four occasions between during November 2009, General Logistics International of New Brunswick, New Jersey, facilitated the unauthorized export of EAR99 steel scrap, valued at \$672,022, from the United States to the People's Steel Mills, located in Pakistan. The People's Steel Mill appears on the BIS Entity List. For each export, General Logistics International arranged for the trucking of the scrap steel from the U.S. exporter's location to the port of export, arranged for the shipping of the scrap steel to People's Steel Mills in Pakistan, and prepared and submitted shipping documentation, part of which indicated that no license was required for these exports. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On January 22, 2015, General Logistics International entered into a settlement agreement with BIS in which it agreed to pay \$90,000.

## Kintetsu World Express (U.S.A.), Inc.

---

**The Violation:** In 2010, Kintetsu World Express (U.S.A.), Inc. (KWE) of East Rutherford, New Jersey, caused, aided and/or abetted an act prohibited by EAR. Specifically, KWE, acting as a freight forwarder, facilitated the export of three spiral duct production machines and related accessories, designated as EAR99 and valued at \$250,000, from the United States to China National Precision Machinery Import/Export Corporation (CPMIEC) in the People's Republic of China without the required U.S. Government authorization. At the time of the export, CPMIEC appeared on the Department of Treasury's Office of Foreign Assets Control Specially Designated Nationals List because it had supplied Iran's military and Iranian proliferators with missile-related dual-use items. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** On September 26, 2014, KWE agreed to pay a \$30,000 civil penalty.

## Rukhsana Kadri / R&A International Trading, Inc.

---

**The Violation:** From in or about October 2009, through at least May 2012, Jamaica, New York-based freight forwarding company R&A International Trading, Inc. dba R&A International Logistics (R&A International), and its president and owner Rukhsana Kadri aka Roxanne Kadri (Kadri), of Davie, Florida, conspired to conceal and misrepresent the identity of the exporter or U.S. Principal Party in Interest (USPPI) on SED or AES records filed with the U.S. Government, and committed a series of related violations, including soliciting a false statement during the course of an investigation. R&A International and Kadri conspired with one of their customers, the actual exporter/USPPI (Customer No. 1), to falsely list another of their customers (Customer No. 2) as the USPPI in SED/AES filings they made in connection with at least 278 exports of computer equipment, involving items totaling approximately \$22 million in value, primarily to trading companies in the United Arab Emirates. The scheme enabled Customer No. 1 to repeatedly export the items anonymously and contrary to the terms of a distribution agreement, and enabled R&A International and Kadri to obtain Company No. 1's substantial forwarding business. When OEE Special Agents began investigating the transactions, R&A International and Kadri not only made a series of false statements to the Special Agents in an attempt to cover up the conspiracy, but also attempted to enlist Customer No. 2 in the conspiracy and solicited Customer No. 2 to make false statements to the Special Agents to conceal the scheme. Customer No. 2, whose name had been falsely listed in the SED/AES filings without its knowledge or consent, refused. This case resulted from an investigation conducted by OEE's New York Field Office.

**The Penalty:** In December 2013, R&A International and Kadri entered into plea agreements with the U.S. Attorney's Office for the Eastern District of New York, admitting to knowingly making false statements in violation of 18 U.S.C. § 305, in connection with a subset of 10 of the false SED/AES record filings that the

New York Field Office had identified, and agreed to forfeit \$125,263. In addition to the forfeiture, R&A International was sentenced in August 2014 to two years' probation, a criminal fine of \$100,000, and a \$4,000 special assessment, and Kadri was sentenced to three years' probation, a criminal fine of \$30,000, and a \$100 special assessment. In July 2015, R&A International and Rukhsana Kadri jointly and severally agreed to pay a civil penalty of \$500,000, of which \$350,000 was suspended during a five-year probationary period, and also agreed to a five-year suspended denial order. In entering into and as part of the settlement agreement, R&A International and Kadri admitted each of the allegations and violations charged by BIS.

# Chapter 4 – Deemed Exports

## Introduction

Most people think of an export as the shipment of a commodity from the United States to a foreign country, but that is only one type of export. Under the EAR, the “release” of “technology” (as defined in the EAR) or source code subject to the EAR to a foreign person in the United States is also “deemed” to be an export to the foreign person’s most recent country of citizenship or permanent residence and may require an export license under the EAR. A release to a foreign person that occurs abroad may require a deemed reexport license. Technology or source code may be released through visual inspection of an item that reveals “technology” or source code to a foreign person or through oral exchanges with a foreign person of technology or source code in the United States or abroad. For example, if a foreign graduate student living in the United States with a valid visa reviews a blueprint or slides as part of a training or internship program with a private company, an export license may be required if a release occurs that reveals technology to the student. As a general matter, in such circumstances, BIS will “deem” the release to be an export (or reexport, if the release occurs abroad) to the foreign person’s most recent country of citizenship or permanent residency

## Criminal and Administrative Case Examples

### Intevac, Inc.

---

**The Violation:** Between January 2007 and August 2007, Intevac, Inc. released technology subject to the EAR to a Russian national working at its Santa Clara, California facility. Specifically, the company released drawings and blueprints for parts, and identification numbers for parts, development and production technology classified as ECCN 3E001 without the required BIS license. Intevac applied for a deemed export license after discovering the initial releases but failed to prevent additional releases of technology while the license application was pending. BIS charged Intevac with knowledge of these additional releases and considered the company’s conduct to be an aggravating factor in the penalty assessment. The company was also charged with one violation related to the unauthorized transmission of the technology to its subsidiary in China. This case resulted from an investigation conducted by OEE’s San Jose Field Office.

**The Penalty:** On February 19, 2014, Intevac, Inc. agreed to pay a \$115,000 civil penalty.

**Voluntary Self-Disclosure:** Intevac voluntarily disclosed the violations and cooperated fully with the investigation.

### Atmospheric Glow Technologies, Inc. / J. Reece Roth

---

**The Violation:** Between January 2004 and May 2006, through Tennessee-based company Atmospheric Glow Technologies, Inc., J. Reece Roth, a Professor Emeritus at the University of Tennessee, engaged in a conspiracy to transmit export controlled technical data subject to the International Traffic in Arms Regulations to foreign nationals from China and Iran. This controlled technical data was related to a restricted U.S. Air Force contract to develop plasma actuators for a military unmanned aerial vehicle. On September 3, 2008, a federal jury in the Eastern District of Tennessee convicted Roth on 18 counts of Conspiracy and Arms Export Control Act violations. This case resulted from a joint investigation conducted by OEE’s Washington Field Office, the FBI, and AFOSI.

**The Penalty:** On July 1, 2009, Roth was sentenced to 48 months in prison and two years of supervised release. In January 2011, the U.S. Court of Appeals for the Sixth Circuit rejected Roth’s appeal and affirmed his September 2008 conviction. In October 2011, the U.S. Supreme Court denied Roth’s petition for a review of the Sixth Circuit ruling. On January 18, 2012, Roth began serving his sentence at the Federal Correctional Institution in Ashland, KY.

## Maxim Integrated Products, Inc.

---

**The Violation:** Between June 2002 and September 2005, Maxim Integrated Products, Inc. (Maxim) of Sunnyvale, California, made 31 unlicensed exports and reexports of national security controlled integrated circuits and related components classified as ECCNs 3A001 and 3E001 to China, Estonia, Russia and Ukraine. In addition, on two occasions, Maxim released controlled technology for the development of electronic components classified as ECCN 5E992 to an Iranian national employee, and classified as ECCN 3A001, to a Chinese national employee without the required BIS license. Maxim applied for a deemed export license for release of technology controlled for national security reasons to the Chinese national, but made a release of the technology to him while the license application was under review. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On October 3, 2008, Maxim agreed to pay a \$192,000 civil penalty.

## Ingersoll Machine Tools

---

**The Violation:** Between November 2003 and January 2007, Ingersoll Machine Tools (IMT) of Rockford, Illinois made seven unlicensed deemed exports of production and development technology for vertical fiber placement machines and production technology for five axis milling machines classified as ECCN 1E001 and 2E002 to Indian and Italian nationals. The technology was controlled for national security and missile technology reasons to India and Italy. The technology was also controlled to India for nuclear nonproliferation reasons. This case resulted from an investigation conducted by OEE's Chicago Field Office.

**The Penalty:** On August 11, 2008, IMT agreed to pay a \$126,000 civil penalty.

## TFC Manufacturing, Inc.

---

**The Violation:** Between March and April 2006, TFC Manufacturing, Inc. (TFC), a Lakewood, California-based aerospace fabrication facility, released U.S.-origin technology for the production of aircraft parts classified as ECCN 9E991 to an Iranian national employee in the United States without the license required under the EAR. This case resulted from an investigation conducted by OEE's Los Angeles Field Office.

**The Penalty:** On May 20, 2008, TFC agreed to pay a \$31,500 civil penalty.



# Chapter 5 – Antiboycott Violations

## Introduction

The Office of Antiboycott Compliance (OAC) administers and enforces the antiboycott provisions of the EAR, which are set forth in Part 760 of the EAR. These regulations prohibit U.S. persons from complying with certain requirements of unsanctioned foreign boycotts, including requirements that the U.S. person provide information about business relationships with a boycotted country or refuse to do business with certain persons for boycott - related reasons. In addition, the EAR requires that U.S. persons report their receipt of certain boycott requests to BIS. Failure to report receipt of certain boycott requests may constitute a violation of the EAR. Under the antiboycott provisions of the EAR, certain foreign subsidiaries of domestic U.S. companies are considered to be U.S. persons. To help members of the exporting community better understand the substance and applications of



*Cathleen Ryan, Director of the Office of Antiboycott Compliance, speaks at the BIS 2014 Update Conference.*

the antiboycott provisions, BIS offers an antiboycott training module through the *BIS Online Training Room*. The information and examples contained in the module illustrate how to identify an antiboycott issue and how to respond in compliance with the EAR. The Training Room also houses a number of pre-recorded webinars covering a variety of topics, including the basics of U.S. export control and deemed exports. The training modules are presented in a video streaming format.

In addition, Supplement No. 2 to Part 766 of the EAR provides guidance regarding BIS's penalty determination process in the settlement of administrative antiboycott cases involving violations of Part 760 of the EAR, or violations of Part 762 (Recordkeeping) when the recordkeeping requirement pertains to Part 760. Similar to guidance regarding administrative export control cases, Supplement No. 2 to Part 766 describes how BIS determines appropriate penalties in settlement of violations in

Antiboycott cases. The guidance contains a comprehensive description of the factors taken into account in determining civil penalties including significant mitigating and aggravating factors.

As in export control cases, BIS encourages submission of voluntary self-disclosures (VSDs) by parties who believe they may have violated the antiboycott provisions of the EAR. The procedures relating to antiboycott VSDs are set out in Section 764.8, which details timing requirements and the information that must be included in the initial notification and in the narrative account of the disclosure.

OAC monitors the type and origin of boycott-related requests received by U.S. persons. Because boycott-related terms and conditions may pose a barrier to trade, OAC partners with the Office of the U.S. Trade Representative and the U.S. Department of State and U.S. Embassy officials to engage with ministers and other government officials in boycotting countries in an effort to remove such boycott language from letters of credit, tenders, and other transaction documents at the source. U.S. companies must still remain vigilant when they undertake any export or other business transactions that might implicate unsanctioned foreign boycotts and report the receipt of requests to comply with such boycotts to BIS, as required by part 760.

For advice concerning boycott-related requests contained in export transaction documents, or any other matter concerning the antiboycott provisions of the EAR, please visit the Office of Antiboycott Compliance portion of the BIS website: <http://www.bis.doc.gov/index.php/enforcement/oac>, or contact the OAC advice line via the website, above, or by telephone at (202) 482-2381.

## **An Overview of the Antiboycott Laws**

### **History**

During the mid-1970s, the United States took steps to counteract the participation of U.S. persons in other nations' economic boycotts of countries friendly to the United States. These actions included the 1977 amendments to the Export Administration Act of 1969 (as carried over into the Export Administration Act of 1979 (EAA) and the Ribicoff Amendment to the 1976 Tax Reform Act. On August 13, 2018, President Trump signed into law the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. §§ 4801-4852, which includes the Anti-Boycott Act of 2018. The ECRA provides the legal authority for BIS's antiboycott enforcement regime.

### **Objectives**

To encourage, and in specified cases, to require U.S. persons to refuse to participate in foreign boycotts that the United States does not sanction. They have the effect of preventing U.S. persons from implementing foreign policies of other nationals that run counter to U.S. policy.

### **Primary Impact**

Although the antiboycott laws are designed to apply to all boycotts of countries that are friendly to the United States imposed by foreign countries, the Arab League boycott of Israelis the principal foreign economic boycott that U.S. persons must be concerned with today.

### **Who is covered by the Laws?**

The antiboycott provisions of the EAR apply to all "U.S. persons," defined to include individuals and companies located in the United States and, in certain circumstances, their foreign affiliates and subsidiaries. These persons are subject to the antiboycott regulations when they undertake certain activities relating to the sale, purchase, or transfer of goods or services (including information) within the U.S. or between the U.S. and a foreign country with the intent to comply with, further, or support an unsanctioned foreign boycott. This includes U.S. exports, forwarding and shipping, financing, and certain other transactions by U.S. persons not in the United States.

## **Administrative Case Examples**

### **RHDC International (Houston)**

---

**The Violation:** During the years 2011 through 2013, in connection with the preparation and processing of documents in Letter of Credit transactions on behalf of its exporter-clients involved in the sale and/or transfer of goods to customers in Kuwait, Lebanon, Qatar and United Arab Emirates, RHDC International LLC (RHDC), located in Houston, Texas, on one occasion received a request to furnish information about the national origin of a United States person and on four occasions received a request to furnish a vessel eligibility certificate signed by other than the owner, master or charterer of the vessel. RHDC failed to report its receipts of these requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

**The Penalty:** On August 11, 2016, RHDC International LLC agreed to pay a civil penalty of \$ 9,000.

## **Vinmar International, Ltd. / Vinmar Overseas, Ltd.**

---

**The Violation:** On seven occasions between 2011 and 2012, two related foreign concerns with Houston, Texas-based U.S. operations, Vinmar International, Ltd. (VIL) and Vinmar Overseas, Ltd. (VOL), furnished prohibited information in bills of lading or vessel certificates regarding the blacklist status or eligibility status of the vessel to enter Arab ports. On ten occasions between 2009 and 2012, the companies failed to report receipt of requests from Lebanon, Libya, Oman, Qatar, Syria, and Yemen to furnish a vessel eligibility certificate signed by other than the owner, master or charterer of the vessel. In addition, on three occasions during 2009, VOL failed to report receipt of a directive from the United Arab Emirates requiring the exclusion of parties of Israeli origin.

**The Penalty:** On September 25, 2015, VOL agreed to pay a civil penalty of \$41,400, and VIL agreed to pay a civil penalty of \$19,800.

## **Baker Eastern, SA (Libya)**

---

**The Violation:** On 22 occasions during the years 2004 through 2008, Baker Eastern, SA (Libya) (Baker Eastern), a controlled-in-fact foreign subsidiary of Baker Hughes, Inc., furnished to Libyan Customs in Libya a Certificate of Origin which contained two items of prohibited information: the first, a negative certification of origin which set out information concerning Baker Eastern's or another person's business relationships with or in a boycotted country; the second, a blacklist certification which set out information concerning Baker Eastern's or another person's business relationships with other persons known or believed to be restricted from having any business relationship with or in a boycotting country. In addition to these 44 violations related to the furnishing of prohibited information, Baker Eastern committed 22 violations on the same occasions by agreeing to refuse to do business with another person pursuant to a requirement or request from a boycotting country. Specifically, the company included a statement in the Certificate of Origin regarding compliance with the principles and regulations of the Arab Boycott of Israel. In total, Baker Eastern committed 66 violations of the antiboycott provisions of the EAR. Baker Eastern voluntarily disclosed these transactions to BIS.

**The Penalty:** On June 12, 2013, Baker Eastern, SA (Libya) agreed to pay a civil penalty of \$182,325.

## **TMX Shipping Company, Inc.**

---

**The Violation:** During the years 2007 through 2010, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to Bahrain, Kuwait, Lebanon and United Arab Emirates, TMX Shipping Company, Inc. (TMX), located in Virginia, on four occasions furnished a statement, signed by other than the owner, master or charterer, certifying that the carrying vessel was eligible to enter, or allowed to enter, the port of destination. In so doing, TMX furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. In addition, on 11 occasions, TMX received a request to furnish a certification by other than the owner, master or charterer of the vessel stating that the vessel was allowed to enter certain ports. TMX failed to report its receipts of these requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

**The Penalty:** On October 31, 2013, TMX Shipping Company, Inc. agreed to pay a civil penalty of \$36,800.

## Laptop Plaza, Inc. (aka IWEBMASTER.NET, Inc.)

---

**The Violation:** In 2006, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to Pakistan and Lebanon, Laptop Plaza, Inc. (Laptop), located in California, on four occasions, furnished to its customer an invoice which set out a statement that the goods were not of Israeli origin and did not contain Israeli materials. Furnishing this information is prohibited because the information concerns Laptop's or another person's business relationships with or in a boycotted country. In addition, on three occasions, Laptop failed to maintain records of transactions relating to a restrictive trade practice or boycott for a five-year period, as required by the Regulations.

**The Penalty:** On September 7, 2013, Laptop Plaza, Inc. agreed to pay a civil penalty of \$48,800.

## Leprino Foods Company

---

**The Violation:** During the years 2009 through 2011, in connection with transactions involving the sale and/or transfer of U.S.-origin goods to consignees in Bahrain, Oman, Qatar and the United Arab Emirates, Leprino Foods Company (Leprino), located in Colorado, on one occasion, furnished a transport certificate, signed by other than the owner, master or charterer, declaring that the ship was permitted to enter the port in Oman, in accordance with the laws of the Sultanate of Oman. By so doing, Leprino furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. In addition, on 15 occasions, Leprino received a request to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott. Among these requests were 12 goods directives indicating that products manufactured or produced in Israel were banned. Leprino failed to report its receipts of these requests to engage in a restrictive trade practice or boycott.

**The Penalty:** On September 16, 2013, Leprino Foods Company agreed to pay a civil penalty of \$32,000.

## AIX Global LLC

---

**The Violation:** In 2008, in connection with a transaction involving the sale and/or transfer of U.S.-origin goods to Iraq, AIX Global LLC (AIX), located in Tennessee, on one occasion agreed to a prohibited condition that the manufacturer must not be a subsidiary of a company included on a list of "Israeli Boycott Companies." By so doing, AIX agreed to refuse to do business with another person, pursuant to an agreement with, a requirement of, or a request from or on behalf of a boycotting country. In the same transaction, AIX furnished prohibited information concerning its or another person's business relationships with another person known or believed to be restricted from having any business relationship with or in a boycotting country. Lastly, AIX, on one occasion, failed to report timely its receipt of requests to take an action which would have the effect of furthering or supporting a restrictive trade practice or unsanctioned foreign boycott.

**The Penalty:** On September 27, 2013, AIX Global LLC agreed to pay a civil penalty of \$15,000 (suspended for six months and thereafter waived, provided AIX committed no violations during the suspension period).





U.S. DEPARTMENT OF COMMERCE  
Bureau of Industry and Security  
Export Enforcement