# Don't Let This HAPPEN TO YOU!

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

September 2016 Edition

**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 2016

**EXPORT ENFORCEMENT**

BUREAU OF INDUSTRY AND SECURITY

U.S. DEPARTMENT OF COMMERCE

# Summary Table of Contents

## Introduction

**Mission and Organization** . . . . . Page 3
Office of Export Enforcement . . . . . Page 4
Office of Enforcement Analysis . . . . . Page 6
Office of Antiboycott Compliance . . . . . Page 7
**Authorities and Remedies** . . . . . Page 7
Criminal and Civil Penalties . . . . . Page 7
Voluntary Self-Disclosures . . . . . Page 9
Denial of Export Privileges . . . . . Page 10
BIS-Administered Lists . . . . . Page 10
Asset Forfeiture . . . . . Page 11
False Statements . . . . . Page 11
**Export Control Reform** . . . . . Page 12
Information Triage Unit . . . . . Page 13
Export Enforcement Coordination Center . . . . . Page 13
Regulatory and Policy Changes . . . . . Page 14
Definition of "Specially Designed" . . . . . Page 15
Policy Developments . . . . . Page 15
**Export Compliance** . . . . . Page 16
Responsible Parties . . . . . Page 16
Nine Principles for an Effective Compliance Program . . . . . Page 16
Transshipments & Re-Exports . . . . . Page 18
Catch-All . . . . . Page 18
Successor Liability . . . . . Page 19
Educational Outreach . . . . . Page 19
Cyber-Intrusions and Data Exfiltration . . . . . Page 19
**Case Presentations** . . . . . Page 20

## Chapter 1 – Terrorism and State Sponsors of Terrorism

**Introduction** . . . . . Page 25
***Criminal and Administrative Case Examples*** . . . . . Page 26
Corezing International PTE, LTD . . . . . Page 26
Antennas and Components / Eric Schneider . . . . . Page 27
Mayrow General Trading Network . . . . . Page 27
Ya Qian "Jonathan" Chen . . . . . Page 28

Sihai Cheng . . . . . Page 28
Susan Yip / Mehrdad Foomanie / Merdad Ansari . . . . . Page 29
Trans Merits Co., Ltd. . . . . Page 29
Schlumberger Oilfield Holdings Ltd . . . . . Page 30
Weatherford International . . . . . Page 30
Robbins & Myers Belgium SA . . . . . Page 31
Engineering Dynamics, Inc. / James Angehr / John Fowler / Nelson Galgoul. . . . . Page 32
Fokker Services B.V. . . . . Page 32
Balli Group . . . . . Page 33
Mozaffar Khazaee. . . . . Page 34
Yavuz Cizmeci . . . . . Page 34
Aviation Services International / Delta Logistics / Neils Kraaipoel / Robert Kraaipoel . . . . . Page 35
Mohammad Tabibi / Michael Edward Todd / Hamid Seifi /
Parts Guys, LLC / Galaxy Aviation Services . . . . . Page 35
EgyptAir Airlines Company . . . . . Page 36
Hetran, Inc. / Helmut Oertmann / FIMCO FZE . . . . . Page 36
Computerlinks FZCO / Infotec / Waseem Jawad / Aramex Emirates LLC . . . . . Page 37
Aiman Ammar / Rashid Albuni / ECC/ATS / iT-Wave FZCO . . . . . Page 37
Barracuda Networks, Inc. and Barracuda Networks Ltd. . . . . Page 38
Ali Reza Parsa. . . . . Page 38
Borna "Brad" Faizy / Touraj Ghavidel / Techonweb . . . . . Page 39
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 39
Springworks Sdn Bhd / Kenneth Chua / Owen Chen . . . . . Page 40
Transamerica Express of Miami Corp . . . . . Page 40
Dani Tarraf / Moussa Hamdan / Douri Tarraf / Hassan Komeiha . . . . . Page 41
Amin Al-Baroudi . . . . . Page 42
Ericsson de Panama S.A. . . . . Page 42

## Chapter 2 – Commerce Control List

**Introduction** . . . . . Page 43
***Criminal and Administrative Case Examples*** . . . . . Page 44
***Nuclear Nonproliferation Controls*** . . . . . Page 44
Xun Wang / PPG Paints Trading (Shanghai) Co., Ltd / Huaxing Construction . . . . . Page 44
Trexim Corporation / Bilal Ahmed . . . . . Page 44
Teledyne LeCroy . . . . . Page 45
Qiang (Johnson) Hu . . . . . Page 45
Nicholas Kaiga. . . . . Page 46
Lisong Ma . . . . . Page 46
Nadeem Akhtar / Computer Communication USA. . . . . Page 46
Mattson Technology Inc. . . . . Page 47

Jirair Avanessian / Farhad Masoumian Amirhossein Sairafi / XVAC . . . . . Page 47
Peter Gromacki / Hamid Reza Hashemi / Amir Abbas Tamimi / Murat Taskiran. . . . . Page 48
***Chemical/Biological Weapons Controls*** . . . . . Page 48
Envirotech Pump Systems, Inc. . . . . Page 48
Flowserve Corporation . . . . . Page 49
Buehler Limited. . . . . Page 49
Dr. Thomas Butler. . . . . Page 50
***Missile Technology Controls*** . . . . . Page 50
Weiss Envirotronics . . . . . Page 50
Ming Suan Zhang . . . . . Page 50
C.A. Litzler Co., Inc. . . . . Page 51
GrafTech International Holdings . . . . . Page 51
Interpoint Corporation . . . . . Page 51
Parthasarathy Sudarshan / Mythili Gopal / Cirrus Electronics, LLC . . . . . Page 52
***National Security Controls*** . . . . . Page 52
Arc Electronics / Alexander Fishenko / Alexander Posobilov / Shavkat Abdullaev / Anastasia Diatlova . . . . . Page 52
Alexander Brazhnikov / ABN Universal . . . . . Page 53
Zhen Zhou Wu / Yufeng Wei /Bo Li / Chitron Electronics, Inc. . . . . Page 53
Daofu Zhang / Jian Guanghou Yan / Xianfeng Zuo / HK Potential Electronics Co. . . . . Page 54
Wind River Systems. . . . . Page 54
Timothy Gormley / Amplifier Research Corporation . . . . . Page 55
ARC International / Yaming Nina Qi Hanson / Harold DeWitt Hanson . . . . . Page 55
Streit USA Armoring, LLC / Streit Middle East / Streit Group FZE / Guerman Goutorov / Eric Carlson . . . . . Page 56
Zhenchun "Ted" Huang . . . . . Page 56
Unisol International. . . . . Page 57
Fu-Tain Lu / Fushine Technology . . . . . Page 57
Jason Liang / Sanwave Electronics . . . . . Page 57
***Crime Controls*** . . . . . Page 58
John Carrington / Sirchie . . . . . Page 58
Lev Steinberg. . . . . Page 58
B&H Foto & Electronics Corp . . . . . Page 59
Vitali Tsishuk / Volha Dubouskaya / Aliaksandr Stashynski / Yahor Osin / Aliaksandr Belski / Ernest Chornoletsky. . . . . Page 59
Boniface Ibe. . . . . Page 59
Mark Komoroski / Sergey Korznikov / D&R Sports Center . . . . . Page 60
Donald Wayne Hatch / Rigel Optics, Inc. . . . . Page 60
Aaron Henderson / Valhalla Tactical Supply . . . . . Page 61
Mike Cabatingan / Romulo Reclusado . . . . . Page 61

## Chapter 3 – Freight Forwarders

**Introduction** . . . . . Page 63
***Criminal and Administrative Case Examples*** . . . . . Page 63
Fulfill Your Packages. . . . . Page 63
Kintetsu World Express . . . . . Page 64
General Logistics International. . . . . Page 64
Federal Express. . . . . Page 64
DPWN Holdings (USA), Inc. (formerly known as DHL Holdings (USA), Inc.) and DHL Express (USA) . . . . . Page 65
R&A International Trading Inc / Rukhsana Kadri . . . . . Page 65
Matthew Kallgren . . . . . Page 66

## Chapter 4 – Deemed Exports

**Introduction** . . . . . Page 67
***Criminal and Administrative Case Examples***. . . . . Page 67
Atmospheric Glow Technologies / J. Reece Roth . . . . . Page 67
Intevac, Inc . . . . . Page 67
Maxim Integrated Products Inc. . . . . Page 68
Ingersoll Machine Tools . . . . . Page 68
TFC Manufacturing, Inc.. . . . . Page 68

## Chapter 5 – Antiboycott Violations

**Introduction** . . . . . Page 69
***Criminal and Administrative Case Examples*** . . . . . Page 70
Vinmar International, Ltd/Vinmar Overseas, Ltd. . . . . Page 70
Baker Eastern, SA (Libya). . . . . Page 71
TMX Shipping Company, Inc.. . . . . Page 71
Laptop Plaza, Inc. (aka IWEBMASTER NET, Inc.). . . . . Page 72
Leprino Foods Company . . . . . Page 72
AIX Global, LLC . . . . . Page 72
RHDC International LLC . . . . . Page 73

# Dear Members of the Exporting Community:

The Obama administration has put in place a new export control system that prioritizes how we use our resources to ensure our export controls protect our national security and foreign policy interests, improve interoperability with our allies, and remove the incentive for foreign manufacturers to stop buying from the United States because of antiquated and cumbersome regulatory requirements. Tens of thousands of military items have now been moved from State Department to Commerce Department jurisdiction. The substance of the President's Export Control Reform or "ECR" initiative has been realized, and these changes represent true reform, resulting in a new 21st century export control system.

The President's ECR initiative has catapulted the Bureau of Industry and Security or "BIS" front and center on the export control stage and cemented our role in advancing this nation's national security and foreign policy interests. This role has been recently characterized by United States Senate Report 114-66: "BIS is the principal agency involved in the development, implementation, and enforcement of export controls for commercial technologies and for many military technologies as a result of the President's export control reform initiative. Export Enforcement…detects, prevents, investigates, and assists in the sanctioning of illegal exports of such items."

This effort could not have succeeded, however, but for the outstanding work and accomplishments of the export control interagency community and the changes they have implemented. We are more secure today because of that work, and we at Export Enforcement at BIS will remain vigilant to safeguard the President's ECR vision, using the many enforcement tools that are available to us. On June 22, 2016, BIS published new Administrative Enforcement Guidelines. The new Guidelines promote greater transparency and predictability to the administrative enforcement process. They also more closely align the administrative enforcement policies and procedures of our Office of Export Enforcement with those of the Office of Foreign Assets Control, both of which administer the bulk of their programs under the International Emergency Economic Powers Act.

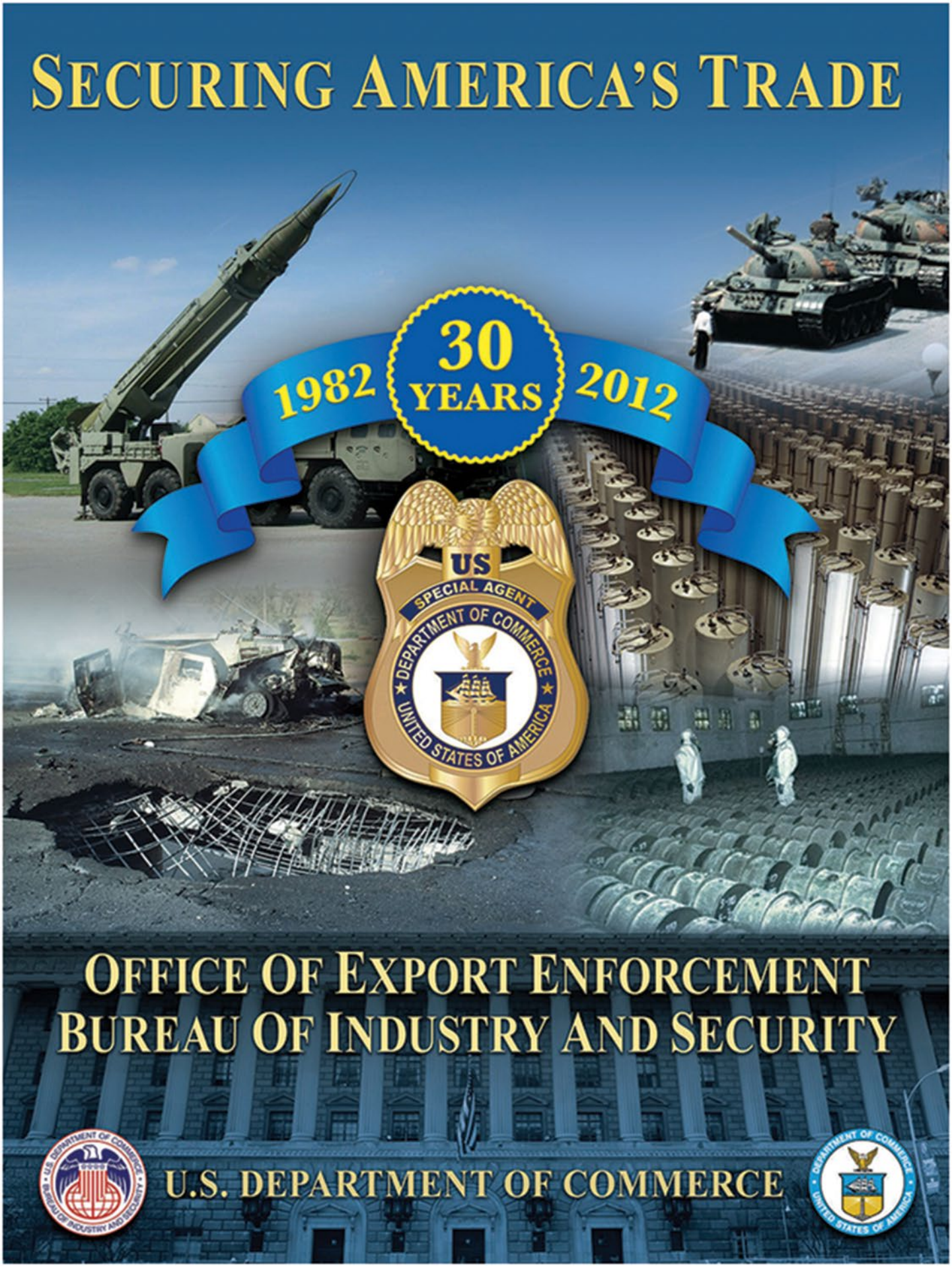
One of our most important objectives at Export Enforcement is to further our partnership with the exporting community to help you comply with the Export Administration Regulations or "EAR." The facilitation of secure trade is in both your financial and reputational interest, and in our mutual national security interest. The partnerships we build with the exporting community are by far the most important. You are our eyes and ears; you are the ones who receive the suspicious inquiries, whose reputation is most damaged when items get diverted, and who spend hard-earned profits on compliance programs while your competitors may not. We ask exporters to be ever-vigilant, as all unsolicited inquiries or unauthorized intrusions, such as cyberthefts or unauthorized access to controlled technology, should trip a compliance system into motion. And we encourage exporters to contact one of our many field locations for advice and support in your compliance endeavors. In addition, our Office of Antiboycott Compliance is available for assistance on compliance with their regulatory requirements as set forth in the EAR, and also works with boycotting countries to remove prohibited language and enable U.S. businesses to compete on an equal footing.

Knowing your customer continues to be at the core of this effort for responsible U.S. companies. Export Enforcement is committed to working with industry to help identify threats, facilitate licensing decisions and party screening, and mitigate penalties where companies have taken the appropriate actions to manage export compliance.

Sincerely,

**David W. Mills**
Assistant Secretary of Commerce for Export Enforcement

# SECURING AMERICA'S TRADE




## 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 International Emergency Economic Powers Act (IEEPA).[1] 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 the 600 series Export Control Classification Number (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.

*Under Secretary for Industry and Security Eric L. Hirschhorn at the Update Conference in Washington, DC, November 2015.*

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 re-exports 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 educating parties to export transactions on how to improve export compliance practices and identify suspicious inquiries, supporting the licensing

[1]Although the Export Administration Act expired on August 20, 2001, the President, through Executive Order 13222 of August 17, 2001, 3 CFR, 2001 Comp., p. 783 (2002), as amended by Executive Order 13637 of March 8, 2013, 78 FR 16129 (March 13, 2013) and as extended by successive Presidential Notices, the most recent being that of August 4, 2016, 81 FR 52587 (August 8, 2016), has continued the Export Administration Regulations in effect under the International Emergency Economic Powers Act (50 U.S.C. § 1701 *et seq.* (2006 & Supp. IV 2010)). BIS continues to carry out the provisions of the Export Administration Act, as appropriate and to the extent permitted by law, pursuant to Executive Order 13222 as amended by Executive Order 13637.

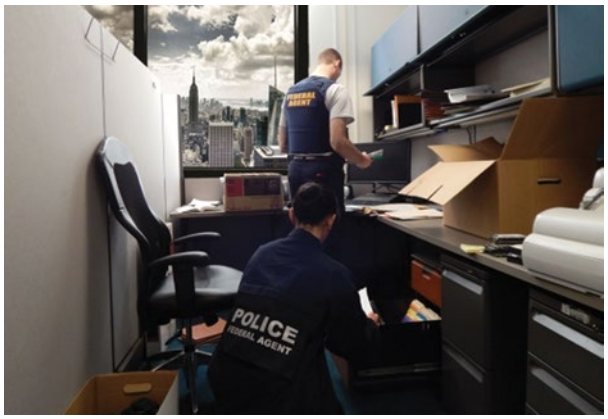
process by evaluating the bona fides of transaction parties, conducting end-use checks, interdicting illegal exports, investigating violations, and referring violators of export control laws for administrative penalties or criminal prosecution. Export Enforcement at BIS has evolved over the past 30 plus 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 President's 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 Houston and Portland. In addition, OEE Special Agents have been deployed to Federal Bureau of Investigation (FBI) field offices in Atlanta, Cincinnati, Minneapolis, Phoenix, San Diego and Salt Lake City, 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 executing a search warrant.*

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 investigation to bring to fruition. 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 re-export 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.[2] For example, OEE works with U.S. Customs and Border Protection to train outbound officers on EAR requirements and 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 and Unverified 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 Export Administration at BIS 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 general prohibitions, end-use or end-user-based controls or proscribed parties).

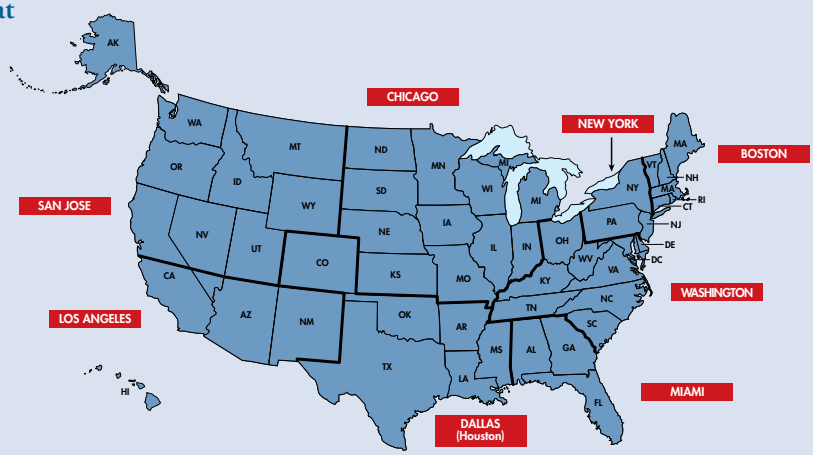
In fiscal year 2015, BIS investigations led to the criminal convictions of 31 individuals and businesses for export violations with penalties of over $156 million in criminal fines, more than $84 million in forfeitures, and 487 months of imprisonment. In addition, OEE and BIS's Office of Chief Counsel completed 47 administrative export matters, resulting in over $15 million in civil penalties. Export Enforcement also initiated the addition of 60 new parties onto the BIS Entity List.

*Director Douglas Hassebrock and Deputy Assistant Secretary Richard Majauskas, at the 33rd Annual National Peace Officer's Memorial Service.*

[2]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.

## WHERE ARE WE LOCATED

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




*www.bis.doc.gov*

**Export Enforcement also has Special Agents co-located with the FBI in Atlanta, Cincinnati, Minneapolis, Phoenix, San Diego and Salt Lake City, 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; 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, re-exports 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." A part of the President's ECR initiative, discussed in more detail below, the ITU is responsible for assembling and disseminating relevant information, including intelligence, 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 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; Moscow, Russia, Frankfurt, Germany; and Singapore. All of these positions have regional responsibilities that extend their reach to an additional 43 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 FY2015, Export Enforcement completed 1,031 end-use checks in 55 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. The case of Arc Electronics (see page 52) demonstrates how collaboration between OEE and OEA helps bring violators to justice. The initial stage of the investigation found a single potentially controlled export of an integrated circuit to Russia. As the investigation developed over a two-year period it was determined that Arc was involved in a complex Russian procurement network supplying microcircuits and other electronic components to Russian military weapons and development programs. OEA analysts provided significant assistance in a variety of ways, including but not limited to: gathering and analyzing SED data; compiling specification data for the components involved; providing preliminary analysis of the specifications to triage components for license determinations; contributing to intelligence information reports produced by the FBI; and finally, assisting in the execution of arrest warrants and collecting evidence.

### *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 re-export transactions.

Under IEEPA, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $284,582 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. (See: Amplifier Research Corp., page 55)

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.

## 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: *http://www.bis.doc.gov/index.php/forms-documents/doc_view/431-part766-administrative-enforcement-proceedings.***

**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
  - Willful or Reckless Violation of Law
  - Awareness of Conduct at Issue
  - Harm to Regulatory Program Objectives
- General Factors
  - Individual Characteristics
  - Compliance Program
- Mitigating Factors
  - Remedial Response
  - Exceptional Cooperation with OEE
  - License Was Likely To Be Approved
- Other Relevant Factors Considered on a Case-by-Case Basis
  - Related Violations
  - Multiple Unrelated Violations
  - Other Enforcement Action
  - Future Compliance/Deterrence Effect
  - Other Factors that OEE Deems Relevant

One of the most significant enforcement tools in the BIS arsenal is our administrative enforcement authorities. On June 22, 2016, BIS published new Administrative Enforcement Guidelines that entered into force on July 22, 2016. The new Guidelines serve to more closely align the administrative enforcement policies and procedures of our Office of Export Enforcement, or "OEE", and the Department of the Treasury's Office of Foreign Assets Control, or "OFAC", both of which administer the bulk of their programs pursuant to International Emergency Economic Powers Act, or IEEPA. The Guidelines reflect several changes to the current Guidelines set forth in Supplement No. 1 to Part 766. First, the Factors set forth in the Guidelines are reconstituted into the following four categories: 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.

Second, the Guidelines will now formally account for the substantial increase in the maximum penalties for violations of IEEPA and distinguish between egregious and nonegregious civil monetary penalty cases. Third, 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.

## *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.[3] 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 fiscal year 2015, OEE opened a total of 382 VSD cases and closed a total of 286 VSD cases. Over half of these VSD cases were closed with the issuance of a warning letter, while nearly a third were closed with "no action" or "no violation."

During fiscal year 2015, we saw a 61 percent increase in VSDs over the previous five years, which can be attributed, in part, to the transfer of ITAR items to the 600 series. Of the 382 VSDs submitted, approximately 70 VSDs involved the CCL's new 600 series commodities. Less than 1 percent of all VSDs were closed with the issuance of administrative sanctions. 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.

[3] See Section764.5 of the EAR for details on how to submit a VSD.

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, re-export, 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 11(h) of the EAA, 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-related statutes. The standard terms of a BIS denial order are published in Supplement No. 1 to Part 764 of the EAR.

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 end-user 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* and are also included in the U.S. Government Consolidated Screening List available at *http://export.gov/ecr.eg_main_023148.asp*.

### Denied Persons List

The Denied Persons List contains the names and addresses of persons subject to a denial of export privileges. Any dealings with a person on this list that would violate the terms of the denial order are prohibited.

### Entity List

The Entity List has evolved into a formidable administrative enforcement tool that prohibits listed foreign persons from receiving some or all items subject to the EAR unless the exporter secures a license. 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 persons. Over 200 persons were added to the Entity List during FY2014 and FY2015 alone.

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 example, T-Platforms, a Russian supercomputer manufacturer, noted that its Entity List designation caused "significant economic and image impact…[because] the decision was interpreted by many manufacturers as a complete ban on the sale of various products to T-Platforms, often not subject to the EAR." BIS removed T-Platforms from the Entity List on December 31, 2013, after T-Platforms cooperated with the U.S. Government and provided assurances that the company would comply with the EAR.

For guidance concerning the prohibitions and license application review policy applicable to a particular person, please review that person's entry on the list. Listed persons 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 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 requirements: all export transactions must be reported in the Automated Export System (AES); license exception-eligibility is suspended; 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. 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, in addition to other penalties. Asset forfeitures prevent export violators from benefiting from the fruits of their crimes, and with no statutory maximum, the value of forfeited assets can greatly exceed criminal fines or civil penalties.

*OEE Special Agents conducting an inspection*

## *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 a Shipper's Export Declaration (SED) or AES Electronic Export Information filing 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, constitute violations of the EAR.

*Law Enforcement Panel presentation at 2015 Update*

## Export Control Reform

In August 2009, President Obama directed a broad-based interagency review of the U.S. export control system with the goal of strengthening national security and the competitiveness of key U.S. manufacturing and technology sectors by focusing on current threats, as well as adapting to the changing economic and technological landscape. As a result of this review, tens of thousands of items have been transferred from the United States Munitions List (USML), administered by the Department of State, to the more flexible licensing regime of the Commerce Control List (CCL). The ECR initiative facilitates interoperability with U.S. allies and partners, strengthens the U.S. defense industrial base by reducing incentives for foreign manufacturers to avoid using U.S. parts and components, and allows the U.S. Government to concentrate its resources on the threats that matter most. The ECR initiative has reduced dramatically the number of time-consuming license applications required for exports to our closest friends and allies, decreasing licensing burdens on U.S. exporters.

Although the majority of the focus has been on the transfer of items from the USML to the CCL, the effort to erect higher fences around those items has been every bit as important. A key piece of this effort involves education. Export Enforcement has conducted hundreds of outreach meetings with companies impacted by the transition of items from the ITAR to EAR. Export Enforcement has also provided training to U.S. Customs

and Border Protection (CBP) on the regulatory changes to facilitate legitimate exports, particularly those eligible for more flexible licensing authorizations. ECR has also established new resources to support U.S. Government evaluation of proposed export transactions and increase interagency coordination in taking enforcement action.

### *Information Triage Unit*

The first of these new resources is the interagency Information Triage Unit (ITU),[4] which helps ensure the overall integrity of our export control system. The ITU, housed within OEA, is responsible for assembling and disseminating relevant information, including intelligence, from which to base informed decisions on proposed exports requiring a U.S. Government license. This multi-agency screening coordinates the reviews of separate processes across the government to ensure that all departments and agencies have a full set of data, consistent with national security, from which to make decisions on license applications. Such screening contributes to more timely, predictable, and consistent processes that U.S. exporters engaged in global trade have confirmed are critical to their competitiveness.

*Then FBI Director Robert S. Mueller, III (right) with Assistant Secretary for Export Enforcement David W. Mills prior to the Director presenting the keynote address at the 2012 Export Control Update Conference in Washington, DC.*

### *Export Enforcement Coordination Center*

As part of the ECR initiative, the President established the Export Enforcement Coordination Center (E2C2) by Executive Order[5] in order to enhance information-sharing and coordination among law enforcement and intelligence officials regarding possible violations of U.S. export control laws. The E2C2 is housed in the Department of Homeland Security (DHS) with the participation of over fifteen federal agency partners, and enables these agencies to better employ their resources in a coordinated effort. The Director of the Center is from DHS; BIS and the FBI provide the two Deputy Directors. The participating agencies include the following:

- U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement
- U.S. Department of Defense, Air Force Office of Special Investigations
- U.S. Department of Defense, Defense Criminal Investigative Service
- U.S. Department of Defense, Defense Intelligence Agency
- U.S. Department of Defense, Defense Security Service
- U.S. Department of Defense, Naval Criminal Investigative Service
- U.S. Department of Energy, National Nuclear Security Administration
- U.S. Department of Homeland Security, Customs and Border Protection

[4] ITU participants include BIS, the Departments of Defense, Homeland Security, Energy, State, and the Treasury, as well as the Intelligence Community.

[5] Executive Order 13558 of November 9, 2010, 75 FR 69573 (November 15, 2010).

- U.S. Department of Homeland Security, Immigration and Customs Enforcement
- U.S. Department of Justice, Bureau of Alcohol, Tobacco, Firearms and Explosives
- U.S. Department of Justice, Federal Bureau of Investigation
- U.S. Department of Justice, National Security Division
- U.S. Department of State, Directorate of Defense Trade Controls
- U.S. Department of the Treasury, Office of Foreign Assets Control
- U.S. Export-Import Bank, Office of the Inspector General
- U.S. Postal Service, Postal Inspection Service
- Office of the Director of National Intelligence, Office of the National Counterintelligence Executive

*Assistant Secretary for Export Enforcement David W. Mills speaking at BIS's 2015 Update Conference*

## *Regulatory and Policy Changes*

Beyond these new compliance and enforcement resources, two regulatory changes to the EAR, driven by the ECR initiative, are of particular benefit to our enforcement efforts – and to the exporting community as described below.

### Strategic Trade Authorization License Exception

License Exception Strategic Trade Authorization (STA) authorizes the export of dual-use and munitions items (including those transferred from the USML to the CCL) to allied and partner nationals subject to

certain safeguards. This License Exception requires that not only the exporter, but also any subsequent re-exporter or transferor, must notify any subsequent consignee of each item shipped under the authority of STA and furnish the Export Control Classification Number (ECCN) of the item. Each consignee must then provide a written statement citing STA, the ECCN, and its agreement to abide by the EAR, including end-use and end-user restrictions, as well as maintain records (for provision to BIS on request). The STA consignee certification requirement thus remains with the item even after re-export or subsequent transfer. For munitions items transferred to the CCL's new "600 series," additional safeguards apply, including limiting applicability to ultimate end-use by the governments of 36 STA-eligible destinations, requiring foreign parties to the transaction to have been previously approved on an export license issued by the Department of State or Commerce, and informing consignees about BIS end-use check requirements. In this way, STA creates a chain of custody and paperwork trail that increases BIS's ability to monitor and enforce EAR compliance. From the perspective of the exporting community, STA will speed up the processing of export transactions previously conducted under license.

### Definition of "Specially Designed"

Another regulatory change under ECR is the new definition of the term "specially designed," which makes compliance efforts more straightforward for the exporting community. The Departments of Commerce and State have established complementary definitions of this term in the ITAR and EAR to specifically articulate objective criteria for determining whether an item is considered "specially designed." This new definition addresses ambiguities resulting from the previous requirement to ascertain "design intent." From an enforcement perspective, this framework clarifies when an item is subject to control as a "specially designed" item.

### Policy Developments

In addition to ECR, BIS's ability to quickly amend our regulations and guidance – from licensing policy to proscribed party lists – ensures that we are addressing the most pressing national security challenges of the day. These actions guide us in our enforcement prioritization, from impeding destabilizing military modernization efforts, such as in Russia and China, to inhibiting Iran's missile and other destabilizing actions, to preventing broader WMD proliferation and terrorist procurement efforts.

On Iran, notwithstanding implementation of the Joint Comprehensive Plan of Action, BIS's export control policy has not changed, and neither has its enforcement posture. Export Enforcement continues to vigorously monitor shipments through the end-use check program to prevent diversions, investigate unauthorized procurements, and alert our international partners about controls that remain on the re-export of U.S.-origin items to Iran. Iran still remains the focus of OEE's enforcement efforts, representing 55 percent of criminal convictions last fiscal year.

*DOC Secretary Penny Pritzker with OEE Deputy Director John Sonderman*

The change in licensing requirements toward Russia following the annexation of Crimea in 2014 is another

example of how regulatory policy directly impacts enforcement priorities. Over the past two years, OEE's caseload for Russia has more than doubled, and 81 names were added to the Entity List in September 2016, to ensure the efficacy of existing sanctions on the Russian Federation for violating international law and fueling the conflict in eastern Ukraine.

In conjunction with our Defense and State Department colleagues, Export Enforcement works with Export Administration to develop industry guidance to prevent the export of U.S.-origin items to locations controlled by ISIS, publishing updates on our website. Export Enforcement has worked directly with international partners to investigate unauthorized exports of spare parts and other items that could be destined for areas controlled by this terrorist organization.

Finally, since President Obama's December 2014 announcement of a new diplomatic and economic policy approach toward Cuba, there has been tremendous interest in exporting and re-exporting to Cuba. The Departments of Commerce and the Treasury have published several sets of regulatory amendments that permit greater opportunities for trade and economic engagement in a wide variety of areas including agriculture, civil aviation, clean energy, and telecommunications. While these amendments remain consistent with the law governing the existing embargo, they reflect the most significant changes in U.S. policy toward Cuba in more than half a century. Most importantly, they create more prosperity for, and a closer relationship between, the people of the United States and Cuba. Of course, Export Enforcement is assisting Export Administration in ensuring U.S exports are made consistent with these regulatory changes.

## 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: Nine 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* under the Compliance and Training tab.

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

- Management Commitment: Senior management must establish written export compliance standards for the organization, commit sufficient resources for the export compliance standards for the organization, commit sufficient resources for the export compliance program, and ensure appropriate senior organizational official(s) are designated with the overall responsibility for the export compliance program to ensure adherence to export control laws and regulations.
- Continuous Risk Assessment of the Export Program.
- Formal Written Export Management and Compliance Program: Effective implementation and adherence to written policies and operational procedures.
- Ongoing Compliance Training and Awareness.
- Pre/Post Export Compliance Security and Screening: Screening of employees, contractors, customers, products, and transactions and implementation of compliance safeguards throughout the export life cycle including product development, jurisdiction, classification, sales, license decisions, supply chain, servicing channels, and post-shipment activity.
- Adherence to Recordkeeping Regulatory Requirements.
- Internal and External Compliance Monitoring and Periodic Audits.
- Maintaining a Program for Handling Compliance Problems, including Reporting Export Violations.
- Completing Appropriate Corrective Actions in Response to Export Violations.

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. The case of Timothy Gormley, a former employee of Amplifier Research, indicates this distinction between individual and corporate responsibility, and is discussed further on page 55.

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 discuss red flags in a section entitled "Know Your Customer," 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 & Re-exports*

Parties to an export transaction cannot bypass the EAR by shipping items through a third country. The transshipment or re-export 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 re-exports 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 re-exports 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. A U.S. company should inquire about such obligations and, where they exist, obtain a copy of any required import license prior to export. Similarly, exporters are required to notify their customers of export license conditions (e.g., requirement for BIS authorization for subsequent transfer (in-country) or re-export) and should make their customers aware that a license (permit) may be required for subsequent re-export from their own government in addition to BIS. In December 2013, BIS published guidance on its website on *Foreign Import/Export License Requirements (Hong Kong/Singapore/United Arab Emirates)* to assist exporters in this regard.

### *Catch-All*

As mentioned in Chapter One, 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 impose 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 three lists described above: 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 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. The case of C.A. Litzler Co., Inc. (page 51) demonstrates the importance of conducting due diligence reviews during the acquisition of a company, or in this particular case, the acquisition of a substantial portion of a company's assets.

### *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 re-export controls, including in cooperation with foreign government partners.

During FY2015, OEE conducted over 1,500 outreaches and tailored its outreach materials to align with the new 600 series requirements. 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. President Obama stated that "[t]he Cyberthreat

is one of the most serious economic and national security challenges we face as a nation. America's economic prosperity in the 21st century will depend on cybersecurity." FBI Director James Comey testified before Congress that "[t]he risk of cyberattacks is likely to exceed the danger posed by al-Qaeda and other terrorist networks as the top national security threat to the United States and will become the dominant focus of law enforcement and intelligence services." 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*. 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.

## Case Presentations

The following cases are referenced in subsequent chapters but are highlighted here as examples of how Export Enforcement at BIS exercises its unique enforcement authorities to ensure the integrity of this nation's export control regime by holding parties accountable for violations of the EAR. As these cases demonstrate, these measures are most often a combination of criminal and civil fines and penalties, and may also include denial of export privileges and placement on the BIS Entity List. The cases are organized based on the reason for control, beginning with Terrorism and State Sponsors of Terrorism, followed by the four multilateral control regimes – Nuclear Suppliers Group; Australia Group (Chemical and Biological Weapons); Missile Technology Control Regime; and the Wassenaar Arrangement, or national security controls, and then by cases pursued in response to violations of controls imposed for crime control and regional stability reasons. Case examples are also presented in subsequent chapters highlighting the importance of the role played by freight forwarders, of controls on deemed exports, and finally cases involving violations of the antiboycott controls.

A recent landmark case for OEE involves Schlumberger Oilfield Holdings, Ltd., a wholly-owned subsidiary of Schlumberger, Ltd., a Curacao-based company (formerly the Netherlands Antilles) with headquarters in Sugarland, Texas. The company entered a plea of guilty in May 2015, and agreed to pay over $232.7 million for conspiring to violate the International Emergency Economic Powers Act by willfully facilitating trade with Iran and Sudan. This case is significant because it puts global corporations on notice that they violate U.S. export laws when they facilitate trade with sanctioned countries from a U.S.-based office, even if they

don't directly ship goods to those sanctioned countries. The criminal penalty represents the largest to date, involving a violation of a sanctions program administered under the International Emergency Economic Powers Act. OEE was the sole investigative agency. Additional details of this case are set forth on page 30.

Another recent development involves the Hetran, Inc. investigation. Hetran, located in Pennsylvania, manufactured a large horizontal lathe, also described as a bar peeling machine, valued at more than $800,000 and weighing over 50,000 pounds. The machine is used in the production of high-grade steel for the manufacture of automobile and aircraft parts. In June 2012, Hetran caused the peeling machine to be shipped from the U.S. to the United Arab Emirates, fraudulently listing a company in the United Arab Emirates as the end-user, knowing that the shipment was ultimately being sent by Iranian company Falcon Instrumentation and Machinery FZE, formerly known as FIMCO FZE (FIMCO), to Iran. In December 2014, Hetran and its President Helmut Oertmann, pled guilty and were both sentenced to probation, and ordered as part of a settlement with BIS to pay a penalty of $837,500 with $500,000 suspended. In July 2015, FIMCO pled guilty and agreed to pay a $837,500 civil penalty with $250,000 suspended. On January 6, 2016, FIMCO was sentenced to a $100,000 criminal fine and a $400 special assessment. The Hetran case features the first time an Iranian company has pled guilty in U.S. District Court in an OEE case. OEA's Export Control Officer in the United Arab Emirates provided considerable assistance in this case. As in the Schlumberger case above, OEE was the sole investigative agency. Additional details of the investigation are set forth on page 36.

OEE has also investigated a number of cases related to U.S.-origin components being used in Improvised Explosive Devices (IEDs) deployed against U.S. and coalition forces in Iraq and Afghanistan. In one case, 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 IEDs in Iraq. Two affiliated individuals extradited to the United States from Singapore pled guilty to criminal charges in the District of Columbia and were sentenced to 37 months and 34 months in prison, respectively. The investigation led to nine indictments and two plea agreements. One of the indicted individuals is currently under arrest in Indonesia under an Interpol Red Notice; extradition of this individual is pending. BIS also added 15 persons located in China, Hong Kong, Iran, and Singapore to the Entity List in connection with the Corezing investigation and prosecution. In a second major IED investigation, OEE investigated the Mayrow General Trading procurement network for obtaining U.S.-origin dual-use and military components for entities in Iran that ended up in IEDs used against Coalition Forces in Iraq and Afghanistan. The Mayrow investigation resulted in the indictment of eight persons and eight companies, the extradition and conviction of a UK national, the arrest of one other individual, and the addition of 75 entities to the BIS Entity List. In 2010, four BIS Special Agents received the Attorney General's Award for Excellence in "Furthering the Interests of U.S. National Security" for this investigation. Export Enforcement at BIS continues to work closely with the Defense Department, particularly the Joint Improvised-Threat Defeat Agency (JIDA), in the fight to counter the impact of IEDs. Additional details of these cases are set forth on pages 26 and 27.

OEE has also investigated a number of cases involving Iran's attempts to acquire commercial aircraft, engines and spare parts. Two major Iranian airlines were designated by the U.S. Department of the Treasury, with Iran Air designated for WMD proliferation and Mahan Air designated for supporting terrorism. The second largest civil penalty levied by BIS was against United Kingdom-based Balli Group PLC and Balli Aviation Ltd. who were penalized $15 million for their role in the illegal export of commercial Boeing 747 aircraft from the United States to Mahan Air and violation of a BIS Temporary Denial Order (TDO). The TDO effectively grounded the 747s by prohibiting transactions by third parties involving these aircraft. When Balli failed to make a timely installment of the civil penalty, the entire amount was made due and payable effective immediately and the $2 million of the civil penalty that had been suspended was also re-imposed. Balli also

pled guilty to two related criminal charges and paid an additional $2 million criminal penalty. Additional details of this case are set forth on page 33.

OEE has also investigated a number of cases where U.S.-origin equipment and technology were used in network infrastructure to monitor and oppress the peoples of Iran and Syria. In December 2011, BIS added two parties to the Entity List based on evidence that they purchased U.S.-origin internet filtering devices and transshipped the devices to Syria. The devices had the potential to be used by the Syrian government to block pro-democracy websites and identify pro-democracy activists as part of Syria's brutal crackdown against the Syrian people. In April 2013, BIS imposed a $2.8 million civil penalty, the statutory maximum, on the UAE firm Computerlinks FZCO related to the same transactions. Additional details of this case are set forth on page 37.

OEE investigated a case involving the first time a Chinese company has pled guilty to an export control violation. In December 2012, China Nuclear Industry Huaxing Construction Co. Ltd. (Huaxing Construction) pled guilty in connection with a scheme to export and transship high-performance epoxy coatings from the United States to the Chashma II Nuclear Power Plant in Pakistan. Huaxing Construction agreed to pay the maximum criminal fine of $2 million, with $1 million suspended. Huaxing Construction also agreed to pay a civil penalty of $1 million. Co-conspirator Xun Wang also pled guilty and was sentenced to 12 months in prison, a $100,000 criminal fine, and one year of probation. Wang also agreed to pay a civil penalty of $200,000 (with another $50,000 suspended), and to be placed on the Denied Persons List. In December 2010, co-conspirator PPG Paints Trading Shanghai pled guilty and agreed to pay the maximum criminal fine of $2 million, serve five years of probation, and forfeit $32,319 to the U.S. Government. PPG Paints Trading Shanghai also agreed to pay a civil penalty of $1 million. Additional details of these cases are set forth on page 44.

The largest civil penalty BIS has ever levied was against Weatherford International Ltd. in Houston, Texas, and four of its subsidiaries who agreed, in November 2013, to pay $100 million, with a $50 million civil penalty paid to resolve the violations charged by BIS, a $48 million penalty paid pursuant to the deferred prosecution agreement, and $2 million in criminal fines paid pursuant to the two guilty pleas. The conduct involved export control violations related to export of oil and gas equipment to Iran, Syria, Sudan, and Cuba, as well as items controlled for nuclear non-proliferation reasons exported to Venezuela and Mexico. Weatherford agreed, as part of the settlement agreement, to hire an unaffiliated third-party expert in U.S. export control laws to audit its compliance with respect to all exports or re-exports to Cuba, Iran, North Korea, Sudan and Syria for calendar years 2012, 2013 and 2014. Weatherford International also entered into an additional deferred prosecution agreement for a term of two years and one of its subsidiaries has pled guilty to violations of the Foreign Corrupt Practices Act (FCPA). This agreement included an additional $87.2 million criminal penalty and $65.6 million in civil fines to the Securities and Exchange Commission. This case demonstrates the close relationship between the FCPA, economic sanctions and export controls, and that those companies with FCPA compliance issues often have issues in regard to compliance with sanctions and export control laws as well. This case began with alleged violations of the FCPA, and expanded to include other violations. The Weatherford investigation was conducted by OEE, working closely with the Department of the Treasury's Office of Foreign Assets Control (OFAC) and the Department of Justice. Additional details of this case are set forth on page 30.

OEE has also dismantled a domestically-based procurement network that was illegally exporting electronic components for use by the Russian military. The owner of Arc Electronics, located in Houston, Texas, pled guilty in September 2015, while three other defendants (all employees of Arc Electronics) were convicted after a month-long trial in October 2015, for illegally conspiring to export and for illegally exporting over $30 million worth of sophisticated technology to Russia. Much of the equipment was destined for military

and intelligence agencies. The Arc Electronics case is significant because while it started out with the discovery of a single shipment of a potentially controlled integrated circuit to Russia, the investigation exposed an entrenched network of foreign nationals in the United States who created a front company for the express purpose of circumventing U.S. export controls. Also of significance is the fact that it was the U.S. business community that provided confidential leads and tips to law enforcement officials that led OEE to identify this front company organization. In connection with the conspiracy, BIS added 165 persons and companies to its Entity List for engaging in this illegal export scheme. Additional details of this case are set forth on page 52.

Finally, when a Pennsylvania company discovered its export control manager, Timothy Gormley, was: 1) altering invoices and shipping documents to conceal the correct classification of amplifiers to be exported so that they would be shipped without the required licenses; 2) listing false license numbers on export paperwork for defense article shipments; and 3) lying to fellow employees about the status and existence of export licenses, the company submitted a voluntary self-disclosure to OEE. That disclosure triggered an investigation that resulted in Gormley being sentenced to 42 months in prison. The company itself entered into a settlement with BIS for a $500,000 civil penalty which was fully suspended because of the voluntary self-disclosure and the company's substantial cooperation with the investigation. Additional details of this case are set forth on page 55.

These cases and many more are more fully set forth in the following chapters, and document the importance of compliance with U.S. export controls to protect our national security and to advance our foreign policy interests. **Don't Let This Happen to You!!!**

# 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[6]. 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 re-exporters are not required to seek separate authorization from BIS for an export or re-export subject both to the EAR and to the Iranian Transactions and Sanctions Regulations (ITSR). If OFAC authorizes an export or re-export, 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 re-export 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

[6] 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 re-export of all items subject to the EAR still require authorization from BIS.

a license for export or re-export. 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.

A prime example of the complementary OFAC and BIS missions is the ING Bank N.V. case, which arose out of ongoing investigations into the illegal exports of goods from the United States to sanctioned countries. From the early 1990s until 2007, ING Bank N.V. of the Netherlands moved more than $2 billion illegally through the U.S. financial system – via more than 20,000 transactions – on behalf of Cuban and Iranian entities subject to U.S. economic sanctions. ING Bank knowingly and willfully engaged in this criminal conduct, which caused unaffiliated U.S. financial institutions to process transactions that otherwise would have been rejected, blocked or stopped for investigation under regulations by OFAC relating to transactions involving sanctioned countries and parties. ING Bank eliminated payment data that would have revealed the involvement of sanctioned countries and entities, including Cuba and Iran; advised sanctioned clients on how to conceal their involvement in U.S. dollar transactions; fabricated ING Bank endorsement stamps to fraudulently process U.S. dollar traveler's checks; and threatened to punish certain employees if they failed to take specified steps to remove references to sanctioned entities in payment messages. The investigation arose out of ongoing investigations by OEE's Boston Field Office, the Federal Bureau of Investigation (FBI), the Internal Revenue Service (IRS), and OFAC into the illegal export of goods from the United States to sanctioned countries, including OEE's investigation of Aviation Services International B.V. (ASI), described on page 35. On June 12, 2012, ING Bank N.V. accepted responsibility for its criminal conduct and agreed to forfeit $619 million to the Justice Department and the New York County District Attorney's Office as part of a deferred prosecution agreement.

Another case set forth below, Schlumberger Oilfield Holdings Ltd., demonstrates how OEE Special Agents conduct criminal investigations of violations of OFAC's regulations, in this instance involving the prohibited provision of services. This case is set forth on page 30.

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*

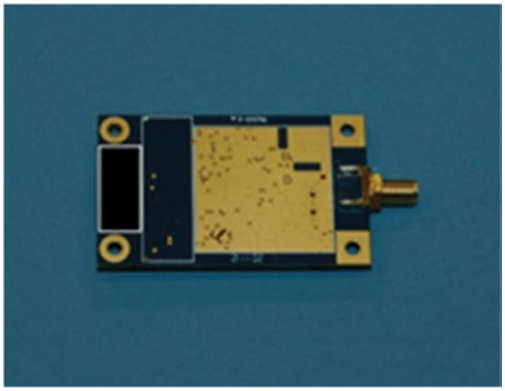
**BIS's website:**
*http://www.bis.doc.gov*

## Criminal and Administrative Case Examples

### 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 U.S. 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 transshipped 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 in U.S. District Court

in the District of Columbia 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. 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, two individuals, Lim Kow Seng and Hia Soo Gan Benson, 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. 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, MA, pled guilty to conspiracy in connection with the export of antennas to end-users in Singapore and Hong Kong without the required 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.

## Mayrow General Trading Network

**The Violation:** Mayrow General Trading, located in the United Arab Emirates, employed a network to illegally procure EAR99 U.S.-origin dual-use and military components for entities in Iran. Such components ended up in improvised explosive devices (IEDs) used against Coalition Forces in Iraq and Afghanistan.[1] This network is spread across several countries, including the United States. U.S.-origin goods diverted to Iran via this network include those controlled by the EAR for missile technology, national security and anti-terrorism reasons as well as those controlled under the

*IED Cache*

[1] On September 22, 2008, BIS removed the entities from the General Order No. 3 relating to Mayrow General Trading and related entities, and added them to the Entity List.

ITAR. This case resulted from an investigation led by OEE's Miami Field Office with the assistance of ICE and DCIS.

**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.

**On October 27, 2010, The Special Agent-In-Charge and three Special Agents of the Miami Field Office received the Attorney General's *Award for Excellence in Furthering the Interests of U.S. National Security* for their efforts in leading the Mayrow investigation.**

## Ya Qian "Jonathan" Chen

**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 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.

## 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 U.S. 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 the People's Republic of 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 U.S. Department of Commerce 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.

## Susan Yip / Mehrdad Foomanie / Mehrdad Ansari

**The Violation:** From October 9, 2007 to June 15, 2011, Susan Yip, a citizen of Taiwan, acted as a broker and conduit for Mehrdad Foomanie of Iran, who bought or attempted to buy items in the United States and arranged to have them unlawfully shipped to Iran through his companies in Iran, Hong Kong, and China. Mehrdad Ansari aka Mehrdad Moeinansari of the United Arab Emirates allegedly attempted to transship and transshipped cargo obtained from the United States by Yip and Foomanie using Ansari's shipping company in Dubai. In her guilty plea, Yip admitted to using her companies in Taiwan and in Hong Kong to carry out the fraudulent scheme. The parts Yip obtained and attempted to obtain for Iran were worth millions of dollars and could be used in military systems such as nuclear weaponry, missile guidance and development, secure tactical radio communication, offensive electronic warfare, military electronic countermeasures, and radar warning and surveillance systems. Foomanie and Ansari remain fugitives. This case resulted from a joint investigation conducted by OEE's Dallas Field Office, the FBI, ICE and DCIS.

**The Penalty:** On October 29, 2012, Yip was sentenced to two years in federal prison. On June 21, 2016, Mehrdad Foomanie, Mehrdad Ansari and related parties including Enrich Ever Technologies Co., Ltd.; Foang Tech Inc.; Global Merchant General Trading L.L.C.; Gulf Gate Sea Cargo L.L.C.; Gulf Gate Sea Cargo LLC; Gulf Gate Shipping Co. L.L.C.; Gulf Gate Spedition GmbH; Hivocal Technology Company, Ltd.; Infinity Wise Technology Limited; Kuang-Su Corporation; Morvarid Shargh Co. Ltd.; Morvarid Sanat Co. LTD; Ninehead Bird Semiconductor; Panda Semiconductor; Pinky Trading Co., Ltd.; Sazgan Ertebat Co. Ltd.; Well Smart (HK) Technology; and Wise Smart (HK) Electronics Limited were added to the BIS Entity List, with a license requirement for all items subject to the EAR with a presumption of denial.

## 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 U.S. 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.

## 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 International Emergency Economic Powers Act. Parent company Schlumberger Ltd. also agreed to the following additional terms during the three-year term of probation (1) 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**

## 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 re-exporting 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 re-export 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 Department of Treasury's Office of Foreign Assets Control, Securities and Exchange Commission, the FBI, the Department of Justice, ICE 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 International Emergency Economic Powers Act 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.

## Robbins & Myers Belgium SA

**The Violation:** In 2006, an internal auditor with Robbins & Myers Inc. (RMI) of Dayton, OH, the U.S. parent company of Robbins & Myers Belgium SA (RMB), discovered that RMI had shipped stators made from U.S.-origin steel to a customer operating oil fields in Syria without obtaining the necessary U.S. government authorizations. These stators, designated EAR99, are important components of oil extraction equipment. The internal auditor informed senior management at RMI of the shipments. Management then confirmed that those shipments had occurred and that they were likely in violation of U.S. law. Although the U.S.-based parent directed RMB to stop such shipments, the subsidiary continued to make three shipments of stators to Syria between August 2006 and October 2006. Following those illegal shipments, employees of the Belgian subsidiary attempted to hide documents related to those shipments from the U.S. government's investigators. On October 2, 2014, corporate officials for National Oilwell Varco, which had acquired in 2013, pled guilty on behalf of RMB. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On October 2, 2014, RMB was ordered to pay a $1 million criminal fine ($250,000 for each of the four counts to which it pled guilty), and to serve a term of corporate probation. As part of its plea agreement, RMB also forfeited $31,716, the gross proceeds received for the four illegal exports. On October 7, 2014, RMB agreed to a $600,000 civil settlement with BIS.

## Engineering Dynamics, Inc. / James Angehr / John Fowler / Nelson Galgoul

**The Violation:** Beginning in March 1995 and continuing through February 2007, James Angehr and John Fowler, owners of Engineering Dynamics Inc., a Louisiana company that produced ECCN 8D992 software to design offshore oil and gas structures, exported and attempted to export software to Iran through a co-conspirator in Brazil without having first obtained the required authorization from the U.S. Government. On April 24, 2008, Angehr and Fowler pled guilty to charges that they conspired to violate U.S. export licensing requirements in connection with this export. Nelson Galgoul, director of the Brazilian engineering company Suporte, acted as an agent for Engineering Dynamics Inc. in the marketing and support of this software and trained users of the software in Iran. On August 2, 2007, Galgoul pled guilty to exporting and attempting to export controlled engineering software to Iran without the required U.S. authorization. This case resulted from a joint investigation conducted by OEE's Houston Resident Office, the FBI and ICE.

**The Penalty:** On August 7, 2008, Angehr and Fowler were sentenced to five years of probation. Angehr was additionally sentenced to six months of confinement in a halfway house, and Fowler was sentenced to four months of confinement in a halfway house. Each defendant was fined $250,000, and ordered to forfeit $218,583. On May 22, 2008, Galgoul was sentenced to 13 months in prison, three years of supervised release, a $100,000 criminal fine, and a $109,291 forfeiture for his part in the conspiracy. On April 18, 2008, Engineering Dynamics, Inc. agreed to pay a civil penalty of $132,791. In addition to the civil penalty paid to BIS, Engineering Dynamics Inc. paid an additional $132,791 to OFAC. Additionally, on December 30, 2011, the Assistant Secretary of Commerce for Export Enforcement issued a Final Order denying Galgoul's export privileges for a period of three years.

## 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 re-export 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 U.S. (and U.K.), 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 International Emergency Economic Powers Act and 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.

## Balli Group

**The Violation:** Beginning in at least October 2007, through July 2008, United Kingdom-based Balli Aviation Ltd. conspired to export three Boeing 747 aircraft, classified under ECCN 9A991, from the U.S. to Iran without first having obtained the required export license from BIS or authorization from the Treasury Department's Office of Foreign Assets Control (OFAC), in violation of the EAR and the Iranian Transactions Regulations. Specifically, Balli Aviation Ltd., through its subsidiaries, the Blue Sky Companies, purchased U.S.-origin aircraft with financing obtained from an Iranian airline and caused these aircraft to be exported to Iran without obtaining the required U.S. government licenses. Further, Balli Aviation Ltd. entered into fictitious lease arrangements that permitted the Iranian airline to use the U.S.-origin aircraft for flights in and out of Iran. In March 2008, BIS issued a temporary denial order (TDO) suspending for 180 days the export privileges of Balli Group PLC (UK) and related companies and individuals, of Blue Airways (Armenia), and of Mahan Airways (Iran), based on evidence that the parties knowingly exported three U.S.-origin aircraft to Iran in violation of the EAR and were preparing to re-export three additional U.S.-origin aircraft to Iran in further violation of the EAR. On February 5, 2010, Balli Aviation Ltd, a subsidiary of the United Kingdom-based Balli Group PLC, pled guilty to the illegal export of commercial Boeing 747 aircraft from the United States to Iran, and to violating the BIS TDO. This case resulted from an investigation conducted by OEE's Washington Field Office.

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

**The Penalty:** On May 11, 2010, Balli Aviation was sentenced to a $2 million criminal fine and corporate probation for five years. On February 4, 2010, Balli Group PLC and Balli Aviation entered a civil settlement with BIS and OFAC, which includes a civil penalty of $15,000,000, of which $2,000,000 was suspended pending no further export control violations. In addition, a five-year denial of export privileges was imposed on Balli Aviation and Balli Group which was suspended provided that during the suspension period neither Balli Aviation nor Balli Group commits any future violations and paid the civil penalty. Under the terms of the settlement Balli Group and Balli Aviation will also have to submit the results of an independent audit of its export compliance program to BIS and OFAC for each of the next five years. To date, both companies have complied with the reporting requirements. On May 19, 2011, the Assistant Secretary for Export Enforcement revoked the suspension of the $2,000,000 civil penalty, based on Balli's failure to make a timely payment of the penalty; and ordered acceleration of the remaining two installment payments totaling $7,200,000 within 15 days of the revocation order.

## Mozaffar Khazaee

**The Violation:** From at least 2009 to 2013, Mozaffar Khazaee, 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 Khazaee 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, Khazaee 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, Khazaee sought to export approximately 1,500 documents containing trade secrets and approximately 600 documents containing highly sensitive defense technology. Analysis of Khazaee's computer media also revealed cover letters and application documents which he sent to multiple state-controlled technical universities in Iran. In those materials, Khazaee 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, Khazaee was arrested at the Newark Liberty International Airport before boarding a flight to return to Iran. Search warrants executed on Khazaee'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. Khazaee 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. Khazaee 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 CBP.

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

## Yavuz Cizmeci

**The Violation:** In June 2008, Yavuz Cizmeci, a Turkish national, aided and abetted his company's transfer of U.S.-origin aircraft to Iran Air without the required authorization and in violation of a Temporary Denial Order. Cizmeci's company, now defunct, was Dunyaya Bais Havacilik Tasimaciligi, also known as Dunyaya Bakis Air Transportation, Ltd. and doing business as Ankair. On June 6, 2008, a Temporary Denial Order was issued naming Ankair, Iran Air and Galaxy Aviation Trade Company Ltd. as denied persons in order to prevent the re-export of a Boeing 747 aircraft to Iran Air. The aircraft was located in Turkey and was in the process of being re-exported or transferred to Iran Air. Despite having notice of the Temporary Denial Order, Cizmeci facilitated the transfer and re-export of the Boeing 747 to Iran Air. Cizmeci submitted false documents to Turkish authorities claiming the aircraft was bound for Pakistan, when in fact it was destined for Tehran, Iran. The Boeing 747 was classified under ECCN 9A991 and was controlled for anti-terrorism reasons. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** On March 23, 2015, the Assistant Secretary for Export Enforcement signed a Final Order imposing a civil penalty of $50,000 and denying Cizmeci's export privileges for 20 years.

## Aviation Services International / Delta Logistics / Neils Kraaipoel / Robert Kraaipoel

**The Violation:** Between October 2005 and October 2007, Aviation Services International BV (ASI), an aircraft supply company in the Netherlands, Robert Kraaipoel, Director of ASI, Neils Kraaipoel, sales manager of ASI, and Delta Logistics received orders from customers in Iran for U.S.-origin aircraft parts and related goods classified under ECCNs 9A991, 1C008, 5A991, and designated EAR99, then contacted companies in the United States and negotiated purchases on behalf of their Iranian customers. The defendants provided false end-user certificates to U.S. companies to conceal the true end-users in Iran. The defendants caused U.S. companies to ship items to ASI in the Netherlands or other locations in the United Arab Emirates and Cyprus; the items were then repackaged and transshipped to Iran. On September 24, 2009, ASI, Robert Kraaipoel and Neils Kraaipoel pled guilty to charges of conspiracy to illegally export aircraft components and other items from the United States to entities in Iran via the Netherlands, UAE and Cyprus. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, ICE and DCIS.

**The Penalty:** On June 12, 2012, Robert Kraaipoel and Neils Kraaipoel were sentenced to five years of probation and a $100 special assessment each. ASI was sentenced to five years of corporate probation, $100,000 criminal fine and a $400 special assessment. In addition, on March 2, 2010, the Assistant Secretary for Export Enforcement signed Final Orders imposing civil penalties of $250,000 (suspended due to the defendants' cooperation) against ASI, Robert Kraaipoel and Neils Kraaipoel, as well as a seven-year denial of export privileges against ASI and Robert Kraaipoel, and a three-year suspended denial of export privileges against Neils Kraaipoel.

## 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 U.S. 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 International Emergency Economic Powers Act. In June 2011, BIS announced the addition of eight indicted defendants located in France, Iran and the United Arab Emirates to BIS's 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.

## 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 re-export 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.

## 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 a $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.

## 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. 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.

## Aiman Ammar / Rashid Albuni / ECC / ATS / iT-Wave FZCO

**The Violation:** Starting in October 2010, Aiman Ammar and Rashid Albuni, both of the United Arab Emirates, implemented a scheme to secure U.S.-origin items for use in the Syrian market through their companies, Engineering Construction and Contracting (ECC) and Advanced Technology Solutions (ATS), both located in Syria, and later iT-Wave FZCO of the United Arab Emirates, to illegally export and re-export web monitoring and controlling equipment and software to Syria, including to the state-run Syrian Telecommunications Establishment. Albuni directly or indirectly provided false destination and end-user information that the items were intended for end-users in such locations as Iraq, Afghanistan, Turkey, Egypt and the United Arab Emirates, when the items were actually intended for Syria. Albuni was involved in negotiating sales, submitting purchase orders and serving as the end-user contact for shipments. Ammar directed payments from his personal and business bank accounts for the unlawful exports or re-exports to Syria. Through this scheme, Ammar and Albuni supplied STE with U.S.-origin computer equipment and software designed for use in monitoring and controlling Web traffic and other associated equipment that they obtained from U.S. companies. Nearly all of the illegally exported and re-exported items were classified under ECCN 5A002 and were controlled for national security and anti-terrorism reasons and as encryption items. This case resulted from an investigation conducted by OEE's San Jose Field Office and ICE.

**The Penalty:** On September 18, 2015, a five-year denial order was imposed against Ammar and a six-year denial order was imposed against Albuni. On the same date, ECC and ATS each received seven-year denial

orders, and iT-Wave FZCO received a four-year denial order. On the same date, the respondents agreed to be held jointly and severally liable for a civil penalty of $7 million, with all but $250,000 suspended for a period of two years.

## 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 re-export 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.

## Ali Reza Parsa

**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 International Emergency Economic Powers Act 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.

## 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, TX, 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.

## 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 U.S. 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.

## Springworks Sdn Bhd / Kenneth Chua / Owen Chen

**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 in U.S. District Court for the Middle District of Florida 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.

## Transamerica Express of Miami Corp.

**The Violation:** From March 2007 through January 2008, freight-forwarders Ulises Talavera, through his Miami, Florida-based firm Transamerica Express of Miami Corp., and Emilio Jacinto Gonzalez-Neira, of Paraguay, through his Miami-based firm, Jumbo Cargo, Inc., exported EAR99 Sony brand electronics to Samer Mehdi, owner of Jomana Import Export, an electronics business located within the Galeria Page, a shopping center in Ciudad del Este, Paraguay. Khaled Safadi of Miami, through his Miami-based firm Cedar

Ditributors, Inc., was a distributor of the electronics to the freight-forwarders. Since December 6, 2006, Galeria Page has been designated as a Specially Designated Global Terrorist entity by the U.S. Department of the Treasury, on grounds that it serves as a source of fundraising for, and is managed and owned by, Hizballah members in the Tri-Border Area. On February 19, 2010, the four individuals and three Miami businesses were indicted in the Southern District of Florida on charges involving the illegal export of electronics to a U.S. designated terrorist entity in Paraguay. On August 18, 2014, Samer Mehdi surrendered to Special Agents from the U.S. Department of Homeland Security who escorted him from Brazil to Miami, FL. On August 19, 2014, Mehdi was arrested upon arrival at the Miami International Airport. On August 19, 2014, Mehdi pled guilty to conspiracy to smuggle goods from the U.S. On September 15, 2010, Gonzalez-Neira and Jumbo Cargo, Inc. pled guilty to conspiracy violations. On October 1, 2010, Safadi and Cedar Distributors, Inc. pled guilty to conspiracy violations, and on October 20, 2010, Talavera and Transamerica Express of Miami Corp. pled guilty to conspiracy violations. This case resulted from a joint investigation conducted by OEE's Miami Field Office and ICE, through an ongoing Organized Crime and Drug Enforcement Task Force.

**The Penalty:** On August 19, 2014, Mehdi was sentenced to one year of probation, a $100 assessment, and forfeited interest in electronics valued at $256,680. On January 24, 2011, Safadi, Cedar Distributors, Inc., Talavera, and Transamerica Express of Miami Corp. were sentenced. Safadi was sentenced to six months of home confinement, six months of probation, and a $100 special assessment. Talavera was sentenced to six months of home confinement, a $100 special assessment, and a shared forfeiture with Cedar Distributors Inc., Transamerica Express of Miami Corp, Gonzalez-Neira, and Jumbo Cargo Inc. of $40,000 worth of seized electronics. Transamerica Express of Miami Corp. was sentenced to three years of probation, a $100,000 criminal fine, a $400 special assessment, and the shared forfeiture. Cedar Distributors was sentenced to three years of probation, a $400 special assessment, and the shared forfeiture. On January 4, 2011, Jumbo Cargo Inc. was sentenced to one year of probation, a $20,000 criminal fine, a $400 assessment, and the shared forfeiture. On January 4, 2011, Gonzalez-Neira was sentenced to 13 months of home confinement, a $100 special assessment, and the shared forfeiture.

## Dani Tarraf / Moussa Hamdan / Douri Tarraf / Hassan Komeiha

**The Violation:** On November 24, 2009, approximately fifteen individuals involved in a Hezbollah procurement network were indicted and arrested in the Eastern District of Pennsylvania. A criminal complaint, unsealed the same day, charged Dani Nemr Tarraf with conspiring to acquire anti-aircraft missiles and possess machine guns. Moussa Ali Hamdan was charged with conspiring to provide material support to Hezbollah, and other defendants – including Douri Nemr Tarraf, and Hassan Mohamad Komeiha - were charged with conspiring to transport stolen goods. The procurement network attempted to supply U.S.-origin commodities subject to the EAR and ITAR to the foreign terrorist organization, Hezbollah, located in Lebanon. The defendants were also charged with false statements on Shippers Export Declarations. The case resulted from a joint investigation conducted by OEE's New York Field Office, the FBI, ICE, IRS, U.S. Secret Service, DCIS, and BATF.

**The Penalty:** On October 27, 2014 and July 19, 2013, two of the defendants were sentenced in U.S. District Court for the Eastern District of Pennsylvania in connection with the violations described above. Two other defendants, Douri Nemr Tarraf and Hassan Komeiha, remain fugitives with outstanding arrest warrants.

## 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 International Emergency Economic Powers Act 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.

## Ericsson de Panama S.A.

**The Violation:** Between 2004 and 2007, Ericsson de Panama S.A. of Panama City, Panama, knowingly implemented a scheme to route items from Cuba through Panama to the United States and back. The scheme included repackaging items to conceal their Cuban origin, forwarding the items to the United States for repair and replacement, and returning the items to Cuba. This scheme involved items classified as 5A002, 4A994, 5A991, and 5B991, controlled for national security, anti-terrorism, and encryption reasons. This case resulted from an investigation conducted by OEE's Dallas Field Office.

**The Penalty:** In May 2012, Ericsson entered into a settlement agreement with BIS in which it agreed to pay $1,753,000 to settle 262 EAR violations. In addition, an independent third party was assigned to conduct an audit of all export transactions connected with Cuban customers undertaken by Ericsson de Panama, its ultimate parent company, or any of its ultimate parent company's other subsidiaries or affiliates.

**Voluntary Self-Disclosure:** By voluntarily disclosing the violations to BIS and the Department of Justice, and cooperating with the investigation, Ericsson was able to avoid criminal prosecution and heavier fines.

# 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. 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.

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

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:*

### 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, re-export 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 the People's Republic of 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.**

### 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

Corp. of Schaumberg, IL, 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 BIS's 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.

## Qiang (Johnson) Hu

**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 to 34 months in prison and $100 special assessment.

## Nicholas Kaiga

**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.

## 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 the People's Republic of China. Ma attempted to export up to five tons of carbon fiber without the required Department of Commerce 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, a Final Order was issued denying Ma's export privileges for a period of ten years.

## 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 International Emergency Economic Powers Act 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.

## Mattson Technology, Inc.

**The Violation:** Between 2006 and 2008, Mattson Technology Inc. of Fremont, California, made 47 unlicensed exports of pressure transducers classified as ECCN 2B230 to customers in Israel, Malaysia, China, Singapore, and Taiwan in violation of the EAR. The pressure transducers, valued at $78,000, were controlled for nuclear non-proliferation reasons. This case cautions manufacturing and distribution partners to pay careful attention to compliance requirements when exporting controlled spare and replacement parts. Penalties assessed related to the unauthorized export of spare and replacement parts can be as costly as those that arise from violations related to the export of complete systems and capital equipment. Companies that authorize spare or replacement part shipments using license exceptions, including for replacement parts and equipment and for temporary exports, must ensure compliance with all of the requirements for authorized use of these exemptions as defined in the Export Administration Regulations. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On April 30, 2012, Mattson Technology agreed to pay $850,000 in civil penalties, $600,000 of which was suspended.

**Voluntary Self-Disclosure:** Mattson Technology voluntarily disclosed the violations and cooperated fully in the investigation.

## Jirair Avanessian / Farhad Masoumian / Amirhossein Sairafi / XVAC

**The Violation:** Between 2007 and 2008, Jirair Avanessian, 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. Avanessian 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, Avanessian and Sairafi re-labeled and undervalued the contents of the shipments in order to mask the true contents and to avoid interception by U.S. officials. In most cases, Avanessian prepared air waybills indicating his shipments contained "spare parts" and that no Shipper's Export Declaration was needed. Avanessian 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, Avanessian 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 Avanessian's export privileges for 10 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 U.S. 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. In order 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.

### *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 10 of its foreign affiliates made unlicensed exports and re-exports 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. Since the penalty was imposed, Flowserve has been an outspoken advocate of U.S. National Security and Foreign Policy. The company has taken a strong stance, both internally and externally, on promoting robust export compliance programs, specifically in the oil and gas industries.

## 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.

### *Missile Technology Controls:*

## 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 the People's Republic of 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 Envirotronic's compliance with U.S. export control laws.

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

## Ming Suan Zhang

**The Violation:** In 2012, Ming Suan Zhang, a citizen of the People's Republic 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 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 International Emergency Economic Powers Act (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 to 57 months in prison, $1,000 forfeiture, and a $100 special assessment.

## 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 Administrative Law Judge 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.

## GrafTech International Holdings Inc.

**The Violation:** Between July 2007 and January 2010, GrafTech International Holdings Inc. (GrafTech), of 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.

## Interpoint Corporation

**The Violation:** During the period 2003-2005, Interpoint Corporation, located in Redmond, Washington, exported EAR99 DC-to-DC converters and/or electromagnetic interference filters to China, with knowledge that the items would be used in Chinese rocket programs. Interpoint also exported such items to the 13th Institute in the PRC, an entity on the BIS Entity List, without the required licenses. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On December 18, 2008, Interpoint Corporation agreed to pay a $200,000 civil penalty.

**Voluntary Self-Disclosure:** The company 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. 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, Parthasarathy 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, Mythili 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:*

## 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. 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.

## Alexander Brazhnikov / ABN Universal

**The Violation:** Alexander Brazhnikov, owner of ABN Universal in Carteret, New Jersey, and his companies are 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 - Acadenucuan E.I. Zababkhinh All-Russian Scientific Research Institute of 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.

## 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, 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.

## Daofu Zhang / Jian Guanghou Yan / Xianfeng Zuo / HK Potential Electronics Co.

**The Violation:** Daofu Zhang, Jiang 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 U.S. 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 Milford, 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 March 7 and March 16, 2016 respectively, Jiang Guanghou Yan and Xianfeng Zuo pled guilty in U.S. District Court for the District of Connecticut in connection with the conspiracy. 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. This case resulted from a joint investigation conducted by OEE's Boston Field Office, the FBI, ICE, DCIS, and the U.S. Air Force Office of Special Investigations.

**The Penalty:** On July 8, 2016, Daofu Zhang was sentenced in U.S. District Court for the District of Connecticut to 15 months in prison and a $63,000 forfeiture.

## Wind River Systems

**The Violation:** Between 2008 and 2011, Wind River Systems of Alameda, California, a wholly-owned subsidiary of Intel Corporation, made 51 exports of encryption software classified under ECCN 5D002, controlled for national security reasons, and valued at a total of nearly $3 million, from the U.S. to end-users in China, Hong Kong, Russia, Israel, South Africa, and South Korea. The end-users of these exports were all government end-users, and a Department of Commerce license was required for these shipments. In addition, on four occasions during the same time period, Wind River made four exports of the software, valued at nearly $28,000, to various entities in China appearing on BIS's Entity List. This case resulted from an investigation conducted by OEE's San Jose Field Office.

**The Penalty:** On October 7, 2014, Wind River Systems agreed to pay $750,000 in civil penalties.

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

## 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 Corp, 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.

## ARC International / Yaming Nina Qi Hanson / Harold DeWitt Hanson

**The Violation:** Between 2007 and 2008, Yaming Nina Qi Hanson (Qi), her husband Harold Dewitt Hanson (Hanson), an employee at Walter Reed Army Medical Center, and a Maryland company, ARC International, LLC, illegally exported miniature Unmanned Aerial Vehicle (UAV) Autopilots to Xi'an Xiangyu Aviation Technical Group in China. On November 13, 2009, Hanson and Qi pled guilty to making false statements. The UAV components are classified as ECCN 9A012 and are controlled for export to China for national security reasons. This case resulted from a joint investigation conducted by OEE's Washington Field Office and the FBI.

**The Penalty:** On February 3, 2010, Hanson and Qi were sentenced in the U.S. District Court in the District of Columbia. Qi was sentenced to 105 days in jail with credit for time served, placed on one year of supervised release, ordered to pay a fine of $250 and a $100 special assessment fee, and ordered to attend a U.S. Department of Commerce sponsored educational training program. Hanson was sentenced to 24 months of probation, ordered to pay a $250 fine and a $100 special assessment, ordered to perform 120 hours of community service, and ordered to attend a U.S. Department of Commerce sponsored training program. On July 16, 2013, Hanson and Qi each also agreed to 15-year Denial Orders against them to settle administrative charges that they made false or misleading statements to U.S. Government agents during the course of an investigation.

## Streit USA Armoring LLC / Streit Middle East / Streit Group FZE / Guerman Goutorov / 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 re-exports 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 re-exported 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 re-export 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 re-exports. 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 Goutorov, 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 re-export 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 re-exported by Streit Group FZE and learning that Streit Group FZE intended to proceed with the Iraq re-export without the required license. Streit USA also had 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 Goutorov, and $50,000 against Carlson. Each of the companies also is required to complete two audits of their compliance programs. All of the respondents are subject to three-year suspended denial orders. The suspensions of portions of the Streit USA and Streit Middle East/Streit Group FZE penalties are subject to a three-year probationary period and related compliance conditions.

## 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 U.S. 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.

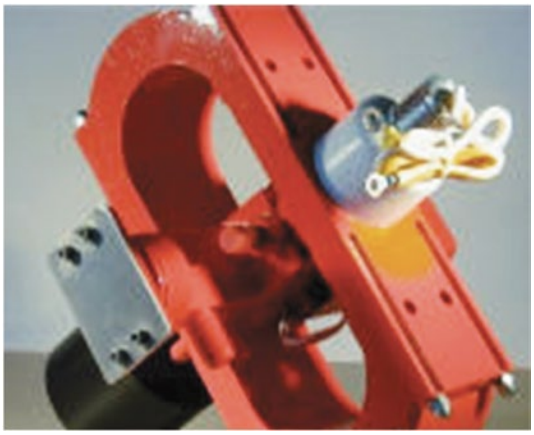
**The Penalty:** On October 20, 2014, Huang was sentenced to 15 months in prison, three years of probation, and a $200 special assessment.

## Unisol International

**The Violation:** From December 31, 2012 through March 25, 2013, Unisol International of Miami, Florida knowingly sold or transferred thermal imaging cameras, items classified under ECCN 6A003 for national security and regional stability reasons and valued at approximately $67,080, to Ecuador and Venezuela. 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.

## Fu-Tain Lu / Fushine Technology



**The Violation:** In 2004, Fu-Tain Lu, owner and operator of Fushine Technology, Inc., a company based in Cupertino, California, facilitated the export of a microwave amplifier to Everjet Science and Technology Corporation, a company in China. The amplifier was classified as ECCN 3A001 and was restricted for export to China for national security reasons. Fushine was an exporter of electronic components used primarily in communications, radar and other applications. On November 17, 2011, Fu-Tain Lu pled guilty in the U.S. District Court in the Northern District of California to violating IEEPA by exporting the microwave amplifier to parties in China without the required export license. This case resulted from a joint investigation conducted by OEE's San Jose Field Office, the FBI, ICE and AFOSI.

**The Penalty:** On October 29, 2012, Lu was sentenced to 15 months in federal prison, three years of supervised release, a fine of $5,000 and ordered to forfeit a seizure valued at $136,000.

## Jason Liang / Sanwave Electronics

**The Violation:** In February 2010, Jason Liang, owner and operator of Sanwave Electronics, of Huntington Beach, California, was arrested and indicted based on charges of attempting to export IR300D infrared cameras to China without the required export licenses from the U.S. Department of Commerce. The items were classified as ECCN 6A003, and were controlled for national security, antiterrorism, and regional stability

reasons. On July 19, 2011, Liang pled guilty in the U.S. District Court in the Central District of California to seven counts of illegal exports. This case resulted from a joint investigation conducted by OEE's Los Angeles Field Office and the FBI.

**The Penalty:** On April 23, 2012, Liang was sentenced in U.S. District Court in the Central District of California to 46 months in prison, three years of supervised release, and a $700 special assessment.

***Crime Controls:***

## John Carrington / Sirchie

**The Violation:** In December 2005, John Carrington, a former North Carolina State Senator, and the former President and Chief Executive Officer of Sirchie Fingerprint Laboratories, a police and forensics equipment supply company based in Youngsville, North Carolina, pled guilty in U.S. District Court to violating IEEPA. This plea arose out of Carrington's involvement in a diversion scheme by which Sirchie Fingerprint Laboratories products, classified as ECCNs 3A981 and 1A985, were shipped through an Italian associate in order to disguise the fact that the items were destined for ultimate end-use in Hong Kong and the People's Republic of China. This diversion scheme was put in place specifically to evade U.S. export control laws. As a result of this plea, Carrington was sentenced to a criminal fine of $850,000 and 12 months of supervised release. He was also placed under a Denial Order by BIS for a period of five years, which barred him from engaging directly or indirectly in any export related activity. Additionally, Sirchie Fingerprint Laboratories was placed under a Five Year Suspended Denial Order and required to pay a total of $400,000 in civil penalties. In January 2008, OEE received information indicating that Carrington was acting in violation of the Denial Order issued against him. A subsequent OEE investigation determined that between February 2006 and November 2007, Carrington was directly involved in Sirchie Fingerprint Laboratories export transactions on ten occasions. His involvement included, among other things, actively assisting in setting prices on products he and other senior members of Sirchie Fingerprint Laboratories management knew would be exported to foreign countries. On January 15, 2008, Raymond James, Inc. formed Sirchie Acquisition Company LLC (Sirchie Acquisition) for the purpose of purchasing essentially all assets of Sirchie Fingerprint Laboratories and several related companies. This case resulted from an investigation conducted by OEE's Washington Field Office.

**The Penalty:** In February 2010, Sirchie Acquisition agreed to enter into a three year deferred prosecution agreement (DPA) with the United States Department of Justice. By entering into this DPA, Sirchie LLC acknowledged that as successor corporate entity, it was responsible for all liabilities of its corporate predecessor, and therefore bore responsibility for the violations of the Denial Order. Sirchie LLC also agreed to pay $2,500,000, the maximum administrative penalty, to BIS for the ten violations, and a five-year Denial Order fully suspended so long as there are no additional export control violations. Additionally, the company agreed to pay a total of $10.1 million in criminal fines and to retain an independent compliance monitor to ensure the company's compliance with the DPA.

## Lev Steinberg

**The Violation:** On September 16, 2009, Lev Steinberg, a resident of Brooklyn, New York, pled guilty to violating the International Emergency Economic Powers Act 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.

## 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 A0987 to a variety of countries, including Russia, Kazakhstan, Hong Kong, Saudi Arabia and South Africa without the required Department of Commerce 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.

## 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 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 ThOR 2 Thermal Imaging Scopes, AN/PAS-23 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 Department of Commerce 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.

## Boniface Ibe

**The Violation:** From November 2003 to August 2010, Boniface Ibe of Mitchellville, Maryland bought 194 shotguns and a .22 caliber handgun from firearm dealers in the Washington, DC and Baltimore metropolitan areas. In September 2010, law enforcement inspected one of Ibe's shipping containers destined

for Nigeria and discovered eight shotguns, one .22 caliber handgun and .22 caliber ammunition concealed in a car inside the container. Shotgun ammunition was found in another vehicle in the container. Dock receipts indicated that an individual in Nigeria was to receive the container, as well as at least four other containers shipped to Nigeria in 2008 and 2009. The handgun and ammunition are controlled under the International Traffic in Arms Regulations and the shotguns are classified under ECCN 0A984 for export by the U.S. Department of Commerce, all of which require a license for export. On February 9, 2011, Ibe pled guilty in U.S. District Court in the District of Maryland to violating IEEPA, illegally exporting defense articles, and delivering a firearm to a common carrier without written notice. This case resulted from a joint investigation conducted by OEE's Washington Field Office, ICE, and the BATF.

**The Penalty:** On July 11, 2011, Ibe was sentenced to five months in prison, 10 months of supervised release, and a $300 special assessment. Ibe is listed on the U.S. Department of State's Debarred List and, pursuant to an order issued by BIS on December 21, 2012, is the subject of a ten-year Denial Order.

## 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 the Departments of State and Commerce. 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.

## Donald Wayne Hatch / Rigel Optics, Inc.

**The Violation:** On July 31, 2008, Donald Wayne Hatch and Rigel Optics Inc. of Washougal, Washington, entered a guilty plea to making false statements and violating the Arms Export Control Act in connection with an illegal export of ITAR-controlled night vision goggles. Hatch and Rigel Optics Inc. sold night vision optical equipment to various foreign customers. This case resulted from a joint investigation conducted by OEE's Chicago Field Office and ICE.

**The Penalty:** On May 12, 2009, Hatch was sentenced to two years of probation and a $5,000 fine with a $100 special assessment for causing false statements to be made on Shipper's Export Declarations. At the same proceeding, a fine of $90,000 and a $400 special assessment was levied against Rigel Optics, Inc. for the

Department of State's Debarred List. On September 7, 2010, BIS issued a 10-year denial order against Rigel Optics, and added Donald Wayne Hatch as a related person, subject to the same denial period.

## Aaron Henderson / Valhalla Tactical Supply

**The Violation:** On September 18, 2009, Aaron Henderson, doing business as Valhalla Tactical Supply of Coralville, Iowa, pled guilty to charges relating to the export of sighting devices classified as ECCN 0A987 to Taiwan and Afghanistan without the required export licenses from the Department of Commerce. This case resulted from a joint investigation conducted by OEE's Chicago Field Office, ICE, and the Drug Enforcement Agency (DEA).

**The Penalty:** On September 18, 2009, Henderson was sentenced to time served followed by two years of supervised release, and a $100 payment to the Crime Victims Fund. On May 28, 2010, a 10 year denial of export privileges was imposed on Henderson and added Valhalla Tactical Supply as a related person.

## 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 International Emergency Economic Powers Act 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 International Emergency Economic Powers Act. 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 the 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.

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

# 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 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

### 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 U.S. or Canada without a U.S. export license. In preparing to export the thermal imaging camera to China, FYP prepared a USPS 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.

## 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.

## 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 U.S. to the People's Steel Mills, located in Pakistan. The People's Steel Mill appears on BIS's 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.

## Federal Express

**The Violation:** Federal Express (FedEx), located in Memphis, Tennessee, was charged with six violations. One two occasions in 2006, FedEx caused, aided and abetted acts prohibited by the EAR when it facilitated the attempted unlicensed export of a PC dialogic board, designated as EAR99, and electronic equipment, classified under ECCN 5A991, from the United States to Mayrow in Dubai, United Arab Emirates. The Mayrow case, set forth on page 27, involved the procurement of electronic components for use in IEDs against U.S. and coalition forces. The exports to Mayrow were thwarted when delivery was halted at OEE's direction. Also, in December 2005, FedEx violated the EAR when it facilitated the unlicensed export of flight simulation software classified under ECCN 4A994 to Beijing University of Aeronautics and Astronautics (BUAA aka Beihang University), an organization on the BIS Entity List. Lastly, FedEx facilitated the unlicensed export of EAR99 printer components from the United States to end-users in Syria. In response to this case, Assistant Secretary for Export Enforcement David W. Mills said, "It is vital that every stakeholder in the U.S. exporting chain remain vigilant in its efforts to prevent prohibited transactions that may be detrimental to our national security, and each will be held accountable if it fails to do so." This case resulted from an investigation conducted by OEE's San Jose, Miami, and Boston Field Offices.

**The Penalty:** On December 2011, FedEx agreed to pay a $370,000 civil penalty.

## DPWN Holdings (USA), Inc. (formerly known as DHL Holdings (USA), Inc.) and DHL Express (USA)

**The Violation:** DPWN Holdings (USA), Inc. (formerly known as DHL Holdings (USA), Inc.) and DHL Express (USA), Inc. (collectively "DHL"), headquarters in Plantation, Florida, unlawfully aided and abetted unlicensed exports to Syria, Iran and Sudan and failed in connection with numerous exports to these countries to comply with recordkeeping requirements of the EAR and OFAC regulations. BIS charged that on eight occasions between June 2004 and September 2004, DHL caused, aided and abetted acts prohibited by the EAR when it transported items subject to the EAR from the United States to Syria, and that with regard to 90 exports between May 2004 and November 2004, DHL failed to retain air waybills and other export control documents required to be retained by the EAR. OFAC charged that DHL violated various OFAC regulations between 2002 and 2006 relating to thousands of shipments to Iran and Sudan. Like DHL's EAR violations, its OFAC violations primarily involved DHL's failure to comply with applicable recordkeeping requirements. This case resulted from a joint investigation conducted by OEE's Miami Field Office and OFAC.

**The Penalty:** In August 6, 2009, DHL agreed to pay a civil penalty of $9,444,744 and conduct external audits covering exports to Iran, Syria and Sudan from March 2007 through December 2011.

## R&A International Trading Inc / Rukhsana Kadri

**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 Shipper's Export Declarations or Automated Export System records ("SED/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 13 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 15, 2016, during the first day of an administrative trial before an administrative law judge, R&A International and Rukhsana Kadri jointly and severally agreed to pay a civil penalty of $500,000, of which $350,000 is suspended during a five-year probationary period, and 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.

## Matthew Kallgren / PC Industries

**The Violation:** In 2008, Matthew Kallgren, sales manager at Powerline Components Industries of Afton, Wyoming, attempted to export EAR99 engine parts to Syria via the United Arab Emirates. The investigation resulted in a criminal plea by Matthew Kallgren and administrative penalties against Kallgren, PC Industries and the freight forwarder, RIM Logistics. This case resulted from a joint investigation conducted by OEE's San Jose Field Office and ICE, with assistance from the FBI and U.S. Customs and Border Protection.

**The Penalty:** Kallgren pled guilty and was sentenced in January 2012 to three years of probation, including four months of home confinement. PC Industries received a deferred prosecution agreement. BIS reached settlement agreements with PC Industries and Kallgren for three-year suspended denial orders. Kallgren agreed to a suspended $75,000 penalty, and the company agreed to a $60,000 penalty. RIM Logistics reached a settlement with BIS for $50,000.

*OEE Special Agents executing a warrant*

# 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 or source code subject to the EAR to a foreign national in the United States is also "deemed" to be an export to the home country or countries of the foreign national and may require an export license under the EAR. A release to a foreign national that occurs abroad may require a deemed re-export license. Technology or source code may be released through visual inspection, oral exchanges of information, or the application to situations abroad of personal knowledge or technical experience acquired in the United States. For example, if a foreign national graduate student living in the United States with a valid visa reviews controlled technology as part of a training or internship program with a private company, an export license may be required because the release of the technology to the student could be considered a "deemed export" to the student's home country. As a general matter, OEE considers a foreign national's most recently acquired immigration status in making home country determinations.

## Criminal and Administrative Case Examples

### 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 ITAR 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.

### 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 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.

## 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 re-exports of national security controlled integrated circuits and related components classified as ECCNs 3A001 and 3E001 to China, Estonia, Russia and the 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 U.S. 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 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.

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

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. The guidance contains a comprehensive description of the factors taken into account by BIS in determining appropriate civil penalties including significant mitigating and aggravating factors in settlement of violations in antiboycott cases.

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 to requests to comply with unsanctioned foreign boycotts and report receipt of such requests 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 adopted two laws to counteract the participation of U.S. persons in other nations' economic boycotts of countries friendly to the United States. These "antiboycott" laws were the 1977 amendments to the Export Administration Act (EAA) (as carried over into the Export Administration Act of 1979) and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA).

### Objectives

The antiboycott laws were adopted 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 Israel is 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

### 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 twenty-two 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 forty-four violations related to the furnishing of prohibited information, Baker Eastern committed twenty-two 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 sixty-six 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 eleven 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 fifteen 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 twelve 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).

## RHDC International, LLC (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.

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