Don't Let This HAPPEN TO YOU!

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

July 2015 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

July 2015

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

Summary Table of Contents

Introduction

Chapter 1 – Terrorism and State Sponsors of Terrorism

Chapter 2 – Commerce Control List

Dear Members of the Exporting Community:

The U.S. Department of Commerce plays an integral role at the intersection of economic growth and national security. The Bureau of Industry and Security (BIS) at the Department of Commerce 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 at BIS detects, prevents, investigates, and assists in the prosecution of illegal exports of such items, with criminal investigators supported by enforcement analysts investigating overseas procurement networks that seek to undermine this Nation's security. In addition, our Office of Antiboycott Compliance works with boycotting countries to remove prohibited language and enable U.S. businesses to compete on an equal footing.

Our most important touchstone is you, the exporting community. You are our eyes and ears; you are the ones receiving the suspicious inquiries; you are the ones whose reputation is damaged when your items get diverted; you are the ones that are spending hard-earned profits on compliance programs while some of your competitors may not be. We ask you to be ever-vigilant, as all unsolicited inquiries or unauthorized intrusions, such as cyberthefts, should trip your compliance systems into motion, and we encourage you to contact one of our field offices for advice. Our commitment to responsible exporters is to help you identify suspicious transactions through a robust outreach program and aggressive use of proscribed parties lists; to give you great weight mitigation if you have an export management and compliance system in place that results in voluntary self-disclosures (VSDs); and to take enforcement action against parties that divert or steal your items without your knowledge.

With regard to VSDs, the number of overall disclosures has increased fifty percent from FY2013 to FY2014. Nonetheless, the outcome of those VSDs has remained fair and consistent. VSDs are a compelling indicator of a party's intent to comply with U.S. export control requirements in the present and the future. BIS's longstanding policy of encouraging the submission of VSDs involving apparent violations is reflected by the fact that, over the past several years, on average only three percent of VSDs submitted have resulted in the imposition of a civil penalty. The vast majority of cases brought to our attention through VSDs result in the issuance of warning letters, containing a finding that a violation may have taken place. 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.

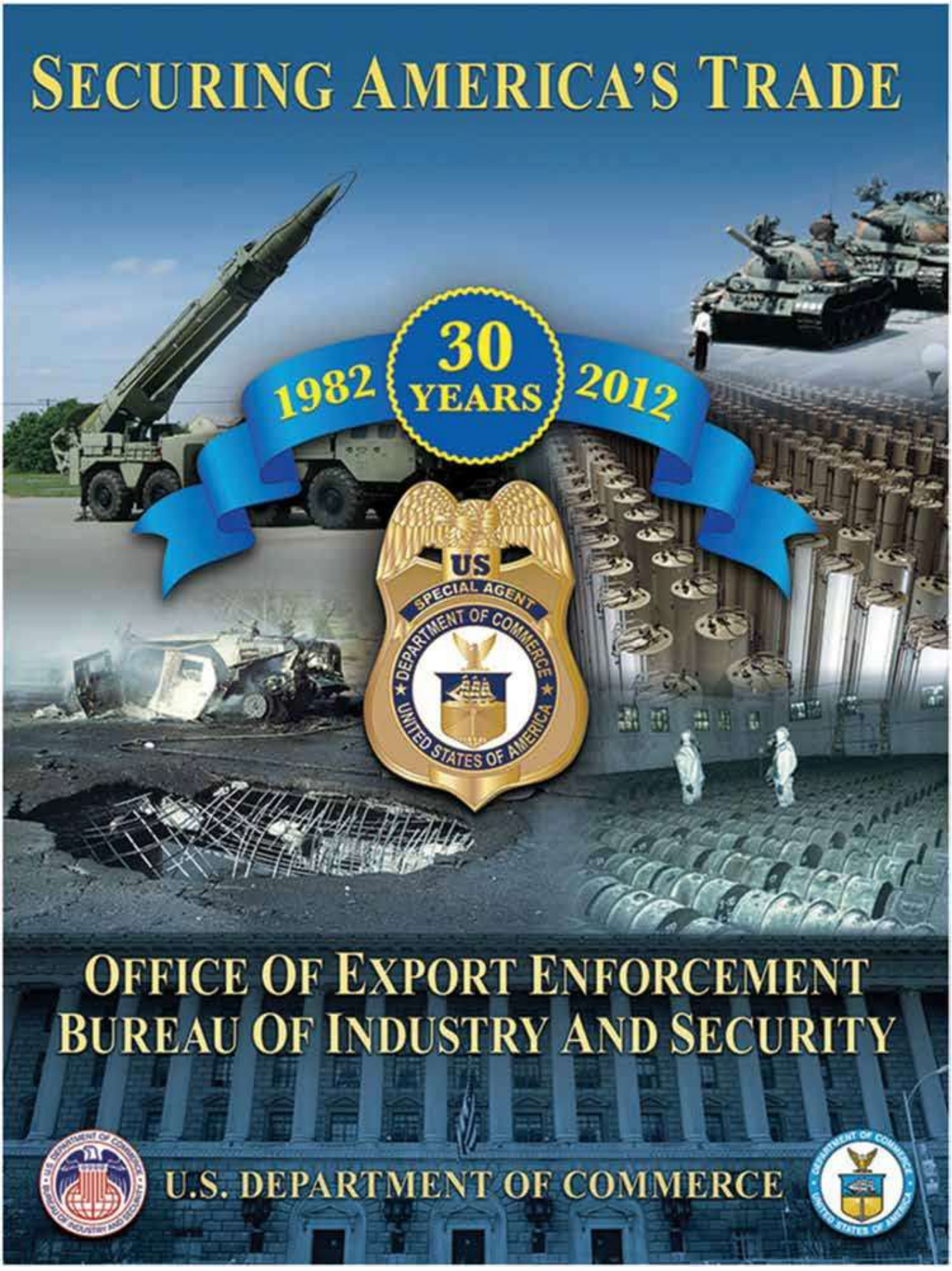
As we finalize the last categories of the USML to CCL transition under Export Control Reform and reflect on recent expansions of controls on unauthorized military end-uses and end-users, it presents an opportunity to reexamine the fundamentals of an effective export compliance program. Knowing your customer 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.

As Under Secretary Hirschhorn has stated, a vigorous enforcement posture on the part of BIS and the larger law enforcement community is only problematic for the individual or company that is purposely trying to flout the law. For those that seek to comply with our export control rules, enforcement is meant to level the playing field, domestically and internationally. I wish you another prosperous year of secure trade!

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

Under Secretary for Industry and Security Eric L. Hirschhorn at the Update Conference in Washington, D.C., July 2014.

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 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 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 is being expanded to cover tens of thousands of munitions items transferring 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.

[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 7, 2014, 79 FR 46959 (August 11, 2014), 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.

Export Enforcement has three program offices: the Office of Export Enforcement, the Office of Enforcement Analysis, and the Office of Antiboycott Compliance. Export Enforcement blends the unique talents of its program offices to channel enforcement efforts against current and emerging threats to national security. 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, D.C., eight field offices located in Boston, Chicago, Dallas, Los Angeles, Miami, New York, San Jose, and Washington, D.C., and a resident office in Houston. In addition, OEE agents have been deployed to Federal Bureau of Investigation (FBI) field offices in Cincinnati, Ohio; Minneapolis, Minnesota; Phoenix, Arizona; Portland, Orgeon; Atlanta, Georgia; and St. Louis, Missouri; 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 the 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 export violations by U.S. persons and the unauthorized reexport or transfer by foreign persons of items subject to the EAR to prohibited end-uses, end-users, or destinations. OEE works closely with other federal law enforcement agencies to identify and act on export violations and with industry to raise awareness of compliance best practices and "red flag" indicators of potential illicit activities.[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 Bureau and Security to bring administrative charges. Export Enforcement also takes actions where appropriate to place parties on the BIS Entity List and Univerified 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

[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.

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, proscribed parties).

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

WHERE ARE WE LOCATED

In addition to our Headquarters at the Department of Commerce in Washington, D.C., Export Enforcement has nine 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, and Washington, D.C.

www.bis.doc.gov

Export Enforcement also has Special Agents co-located with the FBI in Cincinnati, Ohio; Minneapolis, Minnesota; Phoenix, Arizona; Portland, Oregon; Atlanta, Georgia; and St. Louis, Missouri, as well as with DCIS in San Antonio, Texas. Export Enforcement also has Export Control Officers (ECOs) in Beijing, China; Hong Kong, China; New Delhi, India; Moscow, Russia; Dubai, UAE; and Singapore.

In fiscal year 2014, BIS investigations led to the criminal convictions of 39 individuals and businesses for export violations with penalties of over $137 million in criminal fines, more than $1 million in forfeitures, and 568 months of imprisonment. In addition, OEE and BIS's Office of Chief Counsel completed 44 administrative export cases, resulting in over $60 million in civil penalties. Export Enforcement also initiated the addition of 155 new parties onto the BIS Entity List.

Office of Enforcement Analysis

The Office of Enforcement Analysis (OEA) supports the identification, prevention, investigation and prosecution of the illegal exports, reexports and transfers of items subject to the EAR 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, Internal 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 Export Control Reform 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 screen 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 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 six strategic overseas locations critical to BIS's mission: Beijing, China; Hong Kong, China; Dubai, United Arab Emirates; New Delhi, India; Moscow, Russia; 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 Trips and U.S. Embassy personnel. In 2013, Export Enforcement completed 1,044 end-use checks in 51 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 44) 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 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 execution of arrest warrants and collecting evidence.

Export Enforcement Panel at the BIS Update Conference on Export Controls and Policy, July 2014

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 where there has been 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 range of unique administrative enforcement authorities including the imposition of civil penalties, denial of export privileges, and placement of individuals and entities on lists that restrict or prohibit their involvement in export and reexport transactions.

Under IEEPA, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $250,000 per violation 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 imposed by BIS. 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 substantial cooperation with the investigation but where the agency nonetheless decides that a suspended penalty should be imposed for its deterrent effect. (See: Amplifier Research Corp., p. 45)

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.

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 offer 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 "great weight" and are treated as considerable more significant than factors that are not so designated.

- General factors for consideration include:
  - Destination of the export
  - Degree of willfulness involved in violations
  - Number of violations
  - Criminal charges
- Mitigating factors include:
  - Voluntary Self-Disclosure of violations ("great weight")
  - Effective export compliance program ("great weight")
  - Cooperation with BIS investigation
  - Assistance to other BIS investigations
  - No previous record of violations
- Aggravating factors include:
  - Deliberate effort to hide or conceal violations ("great weight")
  - Serious disregard for export compliance responsibilities ("great weight")
  - Item is significant due to its sensitivity or reason for control ("great weight")
  - History of violations
  - High quantity of value of exports

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] BIS 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 Export Enforcement determine the issuance of an administrative penalty is appropriate for the resolution of a VSD, "great weight" is accorded the VSD in assessing and mitigating the penalty. In appropriate cases, fines, and other administrative penalties may be significantly reduced and/or suspended for a probationary period. During fiscal year 2014, OEE opened a total of 312 VSD cases and closed a total of 213 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." Only a very few, around three percent, were closed with the issuance of administrative sanctions. In addition, during fiscal year 2014, approximately 90 VSDs involving the CCL's new 600-series commodities were submitted.

Denial of Export Privileges

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

Denial of export privileges may be imposed as part of an administrative penalty. Under Section 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 form 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*.

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

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. 340 persons were added to the Entity List during FY2013 and FY2014 alone.

The Entity List is also a marketing incentive for 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 cooperating with the U.S. Government and receiving 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 require removal from the Entity List by submitting a request pursuant to 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 a market 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 on 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 BIS are statements on a Shipper's Export Declaration or AES Electronic Export Information filing that an export is destined for one country when it is really destined for a sanctioned destination, the export does not require a license (i.e., that is "NLR") when in fact a license is required for the shipment, false item valuations and 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.

Export Control Reform

Secretary Pritzker at BIS's 2013 Update Conference describing how Export Control Reform simplifies controls on less significant military items that have the same utility as their commercial variant, as demonstrated by certain military and commercial aircraft switches.

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 are now being 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 will facilitate interoperability with U.S. allies and partners, strengthen the U.S. defense industrial base by reducing incentives for foreign manufacturers to avoid using U.S. parts and components, and allow the U.S. Government to concentrate its resources on the threats that matter most. The ECR initiative already is reducing 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 the Customs and Border Protection (CBP) on the regulatory changes to facilitate legitimate exports, particularly those eligible for more flexible licensing authorizations.

In addition to the newly revamped Unverified List referenced above, 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.

Export Enforcement Coordination Center

As part of the ECR, 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
- U.S. Department of Homeland Security, Homeland Security Investigations
- 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

[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 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 2013 Update Conference.

Regulatory Changes

In addition to 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.

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 reexporter 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 reexport or subsequent transfer. For munitions items transferred to the CCL's new "600 series," additional safeguards apply, including limiting applicability for 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.

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. They 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 Supplements 1 and 2 to Part 766 of the EAR, an effective compliance program is entitled to great weight 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 will afford great weight 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 45.

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, 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.

Transshipment & Reexports

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

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

In addition, exporters should be knowledgeable about the export control requirements of their customers and are strongly encouraged to obtain copies of any relevant import licenses (permits) prior to export. For example, Hong Kong requires all importers to receive a license prior to receipt of multilaterally-controlled items from abroad. 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 reexport) and should make their customers aware that a license (permit) may be required for subsequent reexport from their own government in addition to BIS. In December 2013, BIS published guidance on its website on *Foreign Import/Export License Requirements (Hong Kong/Singapore)* 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 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 Terrorists, 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 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 (p. 42) 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 and review compliance best practices, and alert them if appropriate of offshore illicit procurement activities that they may be a target of. Export Enforcement also engages American business communities' overseas and foreign trade and industry associations to promote awareness of U.S. export and reexport controls, including in cooperation with foreign government partners.

During 2014, OEE conducted over 1,300 outreaches and tailored our 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 over the past year, where we alert companies of suspicious parties that may be seeking to obtain sensitive items. We fully appreciate 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. To expand further, it is becoming almost a daily occurrence to read about a cyber-intrusion or attack. President Obama recently 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 cyber-attacks 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, 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.

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, D.C.

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 effectively 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 brings 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, as well as 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. exports laws when they facilitate trade with sanctioned countries from a U.S.-based office building, even if they don't directly ship goods to those sanctioned countries. The criminal penalty represents the largest to date in a sanctions investigation administered under the International Emergency Economic Powers Act. OEE was the sole investigative agency.

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. 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. Details of the investigation are set forth on page 24.

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. The investigation led to nine indictments and two plea agreements. One of the indicted inviduals is currently under arrest in Indonesia under an Internpol 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 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 Explosive Device Defeat Organization (JIEDDO) in the fight to counter the impact of IEDs.

OEE has also investigated a number of cases involving Iran's attempts to acquire commercial aircraft, engines and spare parts. The two major Iranian airlines have been designated by the U.S. Department of the Treasury, with Iran 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 fined $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 foreign persons involving these aircraft. When Balli failed to make an 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.

OEE has also investigated a number of cases where U.S.-origin equipment and technology was 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, which was the statutory maximum, on the UAE firm Computerlinks FZCO related to the same transactions.

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.

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 enter into a deferred prosecution agreement and pay a combined $100 million for export control violations related to export of oil and gas equipment to Iran, Syria, Cuba and other countries. BIS also alleged that Weatherford exported items controlled for nuclear non-proliferation reasons 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 of reexports to Cuba, Iran, North Korea, Sudan and Syria for calendar years 2012, 2013 and 2014. On January 17, 2014, in the Southern District of Texas, two of Weatherford International's subsidiaries pled guilty to a one-count information filed on the Foreign Corrupt Practices (FCPA) investigation with a fine of $420,000 and two separate one-count informations on the sanctions violations, with fines totaling $2 million. 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.

Finally, when a Pennsylvania company discovered their export control manager, Timothy Gormley, was 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; listing false license numbers on export paperwork for defense article shipments; and 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.

These cases and other 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 casesas a consequence of their designation by the Secretary of State as state sponsors of terrorism. As of the date of publication of this manual, 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 Cubaand North Korea[6]. As a practical matter, many export 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.

In 2012, OFAC renamed the Iranian Transaction Regulations as the Iranian Transaction and Sanctions Regulations (ITSR), and amended them to implement enhanced controls with respect to knowing reexports by foreign persons owned or controlled by U.S. persons. The ITSR authorize the imposition of liability on U.S. persons for knowing reexports to Iran by foreign persons under their ownership or control in violation of the EAR.

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

[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 reexport of all items subject to the EAR still require authorization from BIS.

reexporters are not required to seek separate authorization from BIS for an export or reexport subject both to the EAR and to ITSR. If OFAC authorizes an export or reexport, such authorization is considered authorization fo purposes of the EAR as well. It is important to note that transactions that are not subject to OFAC regulatory authority may require BIS authorization. No person may export or reexport any item that is subject to the EAR if such transaction is prohibited by the ITSR and not authorized by OFAC. This prohibition applies whether or not the EAR independently require a license for export or reexport. Please see section 746.7 of the EAR or visit *http://www.bis.doc.gov/index/php/policy-guidance/country-guidance/sanctioned-destinations/iran* for more information.

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 19902 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 transaction – 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 BIS'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 29. 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.

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

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). 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 train properly 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 BIS'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.

Ya Qian "Jonathan" Chen

The Violation: Ya Qian Chen, a/k/a Jonathan Chen, pled 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, NV, 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 BIS'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.

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 f/k/a 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 f/k/a 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 BIS's Houston Resident Office, Department of Justice, Department of Treasury's Office of Foreign Assets Control, Securities and Exchange Commission, FBI, 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.

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 BIS's New York Field Office.

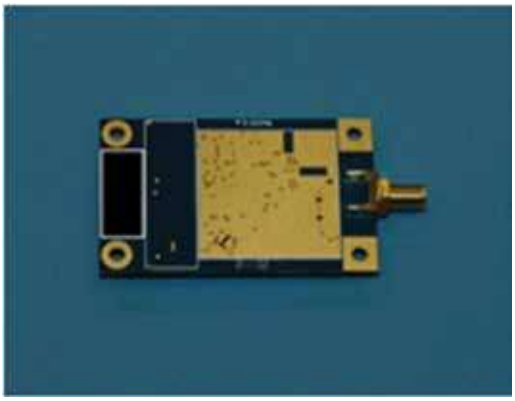
The Penalty: On December 3, 2014, Oertmann and Hetran were each sentenced to 12 months of probation and a $100 assessment. On the same date, they agreed to be held jointly and severally liable for a civil penalty of $837,500 in BIS's related administrative conspiracy case. BIS suspended $500,000 of this 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 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.

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 controlled 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 BIS's Chicago and Boston Field Offices, ICE and the FBI.

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 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.



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.

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

IED Cache

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 this investigation.

[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.

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 BIS'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.

One of the aircraft exported to Iran by the Balli Group, at al.[8]

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, controlled 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 BIS's Washington Field Office.

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.

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 BIS'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.

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 controlled under ECCN 5A992 and controlled 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 BIS's Dallas Field Office and ICE, the FBI, and Defense Criminal Investigative Service (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.

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. 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 BIS'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.

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 Distributors, 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 BIS'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.

Saeed Talebi

The Violation: Saeed Talebi, an Iranian national, worked with others to ship EAR99 industrial parts and goods, including a liquid/air separator, flame detector, motion sensor, pressure transmitter, circuit board, valves, connectors, and other miscellaneous parts, through Germany, Turkey and the United Arab Emirates to various petrochemical companies in Iran. In the course of his scheme, Talebi also caused money to be wired to the United States, including over $300,000 that was sent to a bank account in Manhattan. On September 26, 2012, Saeed Talebi pled guilty in Manhattan federal court to conspiring to illegally export parts and goods designed for use in industrial operations from the U.S. to Iran. This case resulted from an investigation conducted by BIS's New York Field Office.

The Penalty: On February 13, 2013, Talebi was sentenced in U.S. District Court in the Southern District of New York to 12 months in prison and a $100 special assessment.

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 BIS'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 will 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.

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 BIS's San

Jose Field Office and ICE, with assistance from U.S. Customs and Border Protection (CBP) and the FBI.

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.

Mohammad Reza Hajian / R.H. 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 controlled 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 BIS'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.

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 controlled under ECCNs 9A991, 1C008, 5A991, and 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 BIS's Boston Field Office and ICE, the FBI, and Defense Criminal Investigative Service (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 BIS'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.

Hossein Ali Khoshnevisrad / MAC Aviation Group

The Violation: From January 2007 through December 2007, Hossein Ali Khoshnevisrad, the general manager of Ariasa, AG in Tehran, Iran, and Skylife Worldwide Sdn. Bhd, in Kuala Lumpur, Malaysia, purchased helicopter engines and advanced aerial cameras for fighter bombers, controlled under ECCNs 7A994, 9A991,

and the Netherlands. Khoshnevisrad and Ariasa caused Mac Aviation Group, a trading company in Ireland, to

5A991, and 1A003, from U.S. firms and illegally exported them to Iran using companies in Malaysia, Ireland, purchase 17 model 250 turbo-shaft helicopter engines from Rolls-Royce Corp. in Indiana for $4.27 million. Mac Aviation allegedly concealed from Rolls-Royce the end-user of the engines, and ultimately 15 of these engines were exported from the U.S. to Iran via Malaysia or Germany. Among the recipients in Iran was the Iran Aircraft Manufacturing Industrial Company, known as HESA, which was designated by the United States as being controlled by Iran's Ministry of Defense and Armed Forces Logistics, involved in Iran's nuclear and ballistic missile program, and providing support to the Iranian Revolutionary Guard Corps. Khoshnevisrad and Ariasa also caused to be exported to Iran 10 aerial panorama cameras from the United States. These cameras were designed for the U.S. Air Force for use on bombers, fighters and surveillance aircraft, including the F-4E Phantom fighter-bomber, which is currently used by the Iranian military. Khoshnevisrad instructed Aviation Services International, B.V. (ASI), a Dutch aviation parts company, to place an order for 10 of these cameras with a U.S. company located in Pennsylvania and to ship them to an address in Iran, falsely stating that the Netherlands would be the final destination for the cameras. On March 14, 2009, Khoshnevisrad was arrested in San Francisco, and pled guilty on July 1, 2009 to conspiracy to export goods (the Rolls Royce engines) to an embargoed nation, and illegally exporting defense articles (aerial panorama cameras) to Iran. This case resulted from a joint investigation conducted by BIS's Boston Field Office, ICE, the FBI, and DCIS.

The Penalty: On June 2, 2010, Khoshnevisrad was sentenced to 15 months in prison for each count, to run concurrently. In addition, in July 2009, MAC Aviation Group and its principals were added to the BIS Entity List.

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 BIS's Houston Resident Office, ICE, and the FBI.

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.

Massoud Habibion / Mohsen Motamedian / Online Micro, LLC

The Violation: From November 2009 to December 2010, Massoud Habibion and Mohsen Motamedian, co-owners of Online Micro LLC in Costa Mesa, California conspired with a company operating in Dubai, United

Arab Emirates, and Tehran, Iran, to procure U.S.-origin EAR99 computers for export to Iran through Dubai without obtaining the required licenses or authorizations from OFAC. Habibion and Motamedian told a government cooperator to lie to law enforcement officials about Iran being the true ultimate destination and counseled him to say the computer-related goods remained in Dubai. The shipments were valued at more than $1.9 million. On February 16, 2012 Habibion and Online Micro pled guilty to conspiracy to illegally export computers from the United States to Iran through the United Arab Emirates. Mohsen Motamedian pled guilty to obstruction of justice. This case resulted from a joint investigation conducted by BIS's Los Angeles Field Office and ICE, with assistance from CBP.

The Penalty: On May 16, 2012, Habibion was sentenced to 13 months in prison and two years of supervised release, and a $100 special assessment. Motamedian was sentenced to time served in prison, three years of supervised release, a $5,000 criminal fine, and a $100 special assessment for obstruction of justice. Online Micro LLC agreed to forfeit $1.9 million seized during the investigation. In a February 22, 2012 administrative settlement, Habibion and Online Micro agreed to a ten-year denial of export privileges, which is suspended pending no further violations of export laws and compliance with the terms of the criminal and civil agreements. Motamedian separately agreed to a $50,000 civil penalty to settle a charge that he solicited an act prohibited by the Regulations.

Farhad Jenabfar

The Violation: In May 2013, Iranian-born Farhad Jenabfar was arrested in connection with his part in a conspiracy to export military items and aircraft components designated as EAR99 from the United States to Iran without obtaining authorization from OFAC in violation of IEEPA, and the ITR. Jenabfar concealed the actual end-user by falsely stating to the U.S. exporter that he was contacting it on behalf of a customer located in the United Arab Emirates. Jenabfar subsequently facilitated the shipment of goods from the United Arab Emirates to Iran. Evidence obtained during the course of the investigation indicates that the end-users were military entities in Iran. This case resulted from a joint investigation conducted by BIS's Chicago Field Office, ICE, and the FBI.

The Penalty: On December 16, 2013, Jenabfar was sentenced to 28 months in prison and a $50,704 forfeiture.

Mark Alexander

The Violation: On September 25, 2013, Mark Alexander, a/k/a Musa Mahmood Ahmed, former owner and president of HydraJet Technology LLC, located in Dalton, GA, was found guilty at trial to conspiracy. Between 2007 and 2008, Alexander participated in and directed others to participate in the export and installation of two water jet cutting systems, designated EAR99, to Iran via the United Arab Emirates without the required export licenses. This case resulted from an investigation conducted by BIS's Miami Field Office.

The Penalty: On January 6, 2014, Alexander was sentenced to18 months in prison, three years of supervised release, and a $100 special assessment.

OEE Special Agents conducting a joint inspection with Customs and Border Protection Officers.

Mostafa Saberi Tehrani

The Violation: During 2010, Mostafa Saberi Tehrani (Saberi) of Milwaukee, WI, knowingly and willfully violated the embargo against Iran by exported a pump seal designated as EAR99 from the United States to Iran without the required license from OFAC. On June 14, 2013, Saberi pled guilty to violating IEEPA. This case resulted from a joint investigation conducted by BIS's Chicago Field Office and ICE.

The Penalty: On September 13, 2013, Saberi was sentenced to two years of probation, 20 hours of community service, and $100 special assessment. On March 19, 2013, Saberi agreed to a five-year denial of export privileges.

AAG Makina

The Violation: In October 2011, AAG Makina, a Turkish company, worked with others to ship EAR99 industrial parts and goods, including a pressure transmitter, positioners, seat rings, and other miscellaneous parts, valued at a total of $47,000 through Turkey to various petrochemical companies in Iran. This case resulted from an investigation conducted by BIS's New York Field Office.

The Penalty: On December 12, 2012, AAG Makina was added to BIS's Entity List. On March 24, 2015, the company entered into a settlement agreement with BIS in which it agreed to pay $23,000.

Trans Merits Co., Ltd.

The Violation: This investigation began in August 2010, when it was learned that Alex Tsai, a listed Specially Designated National (SDN), had a son named Gary Tsai who lived in the Chicago, IL area and may be involved in providing, or attempting to provide, financial, technological, or other support for, the illegal sale of EAR99 milling machines to his father. Alex Tsai and his company, Trans Merits of Taiwan, were placed on OFAC's SDN List 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 by President George W. Bush in June 2005. As a result of undercover contacts with Gary, email search warrants and evidence were obtained that supported the issuance of arrest warrants for Gary and Alex Tsai. In May 2013, Alex was arrested in Estonia and was later extradited to the United States; simultaneous to Alex's arrest in Estonia, Gary was arrested at his residence. In October 2014 Alex pled guilty, and in December 2014, Gary pled guilty in connection with the illegal export scheme. This case resulted from a joint investigation conducted by BIS's Chicago Field Office, ICE, and the FBI.

The Penalty: On April 24, 2015, Gary Tsai was sentenced to three years of probation and a $100 special assessment. On March 16, 2015, Alex Tsai was sentenced to two years of prison and a $100 special assessment.

Hasan Ibrahim

The Violation: On July 3, 2013, Hasan Ibrahim of Los Gatos, CA, was convicted by a federal jury for numerous violations related to the attempted smuggling of EAR99 hazardous materials to Saudi Arabia. Ibrahim willfully attempted to ship nine different unlabeled hazardous materials, which were intended to be placed on a Lufthansa passenger airplane bound for Frankfurt, Germany. Due to their dangerous properties, two of the chemicals were forbidden to be transported on any aircraft. Ibrahim was also convicted for failure to file export information through the Automated Export System. This case resulted from a joint investigation conducted by the BIS's San Jose Field Office, the FBI, CBP, the U.S. Department of Transportation Office of Inspector General, and the Federal Aviation Administration.

The Penalty: On February 21, 2014, Ibrahim was sentenced 30 days in prison, three years of probation and a $2,200 special assessment.

Sunrise Technologies and Trading Corporation / Jeng Shih

The Violation: From 2007 through 2010, Jeng Shih, a U.S. citizen and owner of Sunrise Technologies and Trading Company of New Hyde Park, New York, conspired with a company operating in the United Arab Emirates to illegally export U.S.-origin computer equipment controlled under ECCN 5A992 through the United Arab Emirates to Iran, without obtaining the required licenses or authorization from OFAC. The defendants caused the illegal export of 526 units of computer-related goods, and later, caused an additional 185 units of computer-related goods to be illegally exported to Iran via the UAE. On October 7, 2011, Shih and Sunrise pled guilty in U.S. District Court in the District of Columbia to conspiracy to violate the International Emergency Economic Powers Act, and to defraud the United States. This case resulted from a joint investigation conducted by BIS's New York Field Office and ICE.

The Penalty: On February 17, 2012, Jeng Shih was sentenced to 18 months in prison, two years of supervised release, a shared forfeiture with Sunrise Technologies of $1.25 million, and a $200 special assessment. Sunrise Technologies was sentenced to two years of corporate probation, the shared forfeiture, and a $200 special assessment. On October 11, 2011, BIS issued Final Orders against Shih and Sunrise imposing a 10-year denial of export privileges (suspended) for their role in the illegal export of the computer equipment to Iran.

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 for regional stability (RS), encryption (EI), communication intercept/surreptitious listening (SL), anti-terrorism (AT), significant items (SI), and crime control and other human rights (CC) reasons.

Criminal and Administrative Case Examples

Nuclear Nonproliferation Controls:

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 and elsewhere using export licenses fraudulently obtained from the Department of Commerce. The pressure transducers are controlled 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 was a joint investigation conducted by BIS'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, controlled under ECCN 1C202, 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 BIS's Chicago Field Office, ICE, and the FBI.

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, a/k/a 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 BIS'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.

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 BIS'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.

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 controlled 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 BIS'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.

Xun Wang / PPG Paints Trading Shanghai / Huaxing Construction

The Violation: From 2006 through 2007, Chinese companies PPG Paints Trading Shanghai Co Ltd, Huaxing Construction Co Ltd., and Xun Wang, Managing Director of PPG Paints Trading, agreed upon a scheme to export, reexport and transship high-performance epoxy coatings from the United States to Chashma II Nuclear Power Plant in Pakistan. The epoxy coatings, designated as EAR99, were transshipped via a third party in 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 BIS'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.

On September 10, 2014, Assistant Special Agent in Charge Jonathan Carson and Special Agents James Fuller and Donald Pearce, 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 Litigative Team in connection with this investigation.

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 Regulations. This case settled following an investigation conducted by BIS'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 controlled 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 BIS's Los Angeles Field Office, the FBI, ICE, CBP, and the Internal Revenue Service-Criminal Investigation Division (IRS-CID).

The Penalty: On July 6, 2011, Avanessian was sentenced to 18 months in prison, three year 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, NY, 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. This case resulted from a joint investigation conducted by BIS's New York Field Office, ICE, and the FBI.

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:

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 as 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 BIS's Dallas Field Office.

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

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

Buehler Limited

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

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.

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 BIS'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 BIS'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 controlled 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 in a joint investigation by BIS'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:

Area S.p.A.

The Violation: In September 2011, Area S.p.A. of Italy transferred and transported items subject to the EAR to Syria without the required U.S. government authorization. Specifically, Area S.p.A. transferred and transported to the Syrian Telecommunications Establishment, an entity affiliated with the Government of Syria, U.S.-origin network performance monitoring items and related U.S.-origin equipment that had been ordered from a company located in the United States. The equipment, valued at $139,694, is classified under ECCN 5A002, and the related equipment is designated as EAR99. The equipment is controlled for national security and anti-terrorism reasons. This case resulted from an investigation conducted by BIS's San Jose Field Office.

The Penalty: On September 11, 2014, Area S.p.A. agreed to pay $100,000 in civil penalties.

Russell Marshall / Universal Industries Limited, Inc.

The Violation: On February 6, 2015, Universal Industries Limited, Inc. (Universal) of Boynton Beach, FL, and its vice president Russell Marshall pled guilty to charges related to the violation of a Department of Commerce Denial Order. Marshall and Universal sold controlled aircraft parts to other U.S. companies with the knowledge that these

companies would export the parts. On July 12, 2012, a three-year denial of export privileges was imposed on Universal and Marshall following their 2011 guilty pleas to violating the Arms Export Control Act, and False Statements, respectively. This case resulted from a joint investigation conducted by BIS's Miami Field Office, ICE, and DCIS.

The Penalty: On April 24, 2015, Marshall was sentenced in U.S. District Court for the Southern District of Florida to 41 months in prison, two years of probation, and a $200 special assessment. On the same date, Universal was sentenced to one year of probation and an $800 special assessment.

Wind River Systems

The Violation: Between 2008 and 2011, Wind River Systems of Alameda, CA, 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.

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 great weight mitigation was given for the company's cooperation during the investigation.

Arc Electronics / Alexander Fishenko / Alexander Posobilov

The Violation: On October 3, 2012, an indictment was unsealed charging members of a Russian military procurement network operating in the United States and Russia, as well as Texas-based Arc Electronics, with illegally exporting high-tech microelectronics from the United States to Russian military and intelligence agencies. Alexander Fishenko, an owner of Arc Electronics, was also charged with operating as an unregistered agent of the Russian government in the United States. The microelectronics allegedly exported to Russia are controlled 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. The defendants allegedly obtained these items by lying and submitting false information regarding the true nature, users, and intended uses of the high-tech items and exporting the items without the required licenses. This case resulted from a joint investigation conducted by BIS's Houston Resident Office, the FBI, DCIS, and Naval Criminal Investigative Service.

The Penalty: While criminal prosecution is ongoing, in October 2012, BIS added 164 foreign persons and companies who received, transshipped, or otherwise facilitated the export of controlled commodities in connection with Arc Electronics to the BIS Entity List. The Entity List prohibits these companies from receiving any item subject to the EAR unless the exporter obtains a BIS license.

Susan Yip / Mehrdad Foomanie / Merdad 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. Merdad Ansari of the United Arab Emirates allegedly attempted to transship and transshipped cargo obtained from the United States by Yip and Foomanie using Ansari's 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 BIS's Dallas Field Office, ICE, the FBI, and DCIS.

The Penalty: On October 29, 2012, Yip was sentenced to two years in federal prison.

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

The Violation: On May 17, 2010, Zhen Zhou Wu, a/k/a Alex Wu, Yufeng Wei a/k/a Annie Wei, and Chitron Electronics, Inc. (Chitron-US), located in Waltham, Massachusetts, were convicted of unlawfully exporting defense articles and Commerce-controlled goods through Hong Kong to China between 2004 and 2007 in violation of U.S. export control laws. Bo Li, a/k/a 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 BIS's Boston Field Office and ICE, the FBI, 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 are listed on the Department of State's Debarred List.

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 BIS'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.

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 BIS'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.

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, which is controlled for national security reasons to parties in China without the required export license. This case resulted from a joint investigation conducted by BIS's San Jose Field Office, ICE, the FBI, and Air Force Office of Special Investigations (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.

Joseph Piquet / Alphatronx, Inc.

The Violation: On five separate occasions from March 2004 through February 2005, Joseph Piquet, President of Alphatronx Inc., of Port St. Lucie, Florida, purchased high-tech, military-use electronic components from a

domestic corporation, and then shipped the items to Hong Kong and the People's Republic of China without first obtaining the required export licenses under the Arms Export Control Act and IEEPA. Among the commodities involved in this conspiracy were high-power amplifiers classified as ECCN 3A001 and designed for use by the U.S. military in early warning radar and missile target acquisition systems, and low noise amplifiers that have both commercial and military use. Piquet submitted false end-use certificates to the manufacturer to conceal the intended final destination of the parts, which he then forwarded through conspirators in Texas and Hong Kong. Piquet was convicted in March 2009 after a four-day trial on all seven counts charged. This case resulted from a joint investigation conducted by BIS's Miami Field Office and ICE.

The Penalty: On May 14, 2009, Joseph Piquet was sentenced to 60 months in prison, two years of supervised release and a $700 special assessment. On May 28, 2010, BIS imposed a ten-year denial order on Piquet, and, in October 2010, added Alphatronx as a related person, making the company subject to the same denial period.

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 BIS'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.

William Tsu / Cheerway Corporation

The Violation: On March 13, 2009, William Tsu of Cheerway Corporation in Hacienda Heights, California, pled guilty to exporting and attempting to export semiconductors and integrated circuits classified as ECCN 3A001 to China without the required export license. This case resulted from a joint investigation conducted by BIS's Los Angeles Field Office, the FBI, ICE, and DCIS.

The Penalty: On August 3, 2009, Tsu was sentenced to 40 months in prison, three years of supervised release, and a $200 special assessment. On February 7, 2011, BIS issued a 10-year Denial Order against Tsu, and added Cheerway Corporation as a related person, subject to the same denial period.

Crime Controls:

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 BIS'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, without a Department of Commerce license. This case resulted from a joint investigation conducted by BIS's New York Field Office, ICE, and the FBI.

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.

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 BIS'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.

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 controlled 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 BIS's Washington Field Office, ICE, and the Bureau of Alcohol, Tobacco, Firearms and Explosives.

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 Sergei 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 BIS'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 BIS'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 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 BIS'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.

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

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

The Violation: In 2010, Kintetsu World Express (U.S.A.), Inc. (KWE) of East Rutherford, NJ, 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 BIS'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, NJ, 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 BIS'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) was charged with six violations. On two occasions in 2006, FedEx, located in Memphis, Tennessee, caused, aided and abetted acts prohibited by the EAR when it facilitated the attempted unlicensed export of a PC dialogic board, designated EAR99, and electronic equipment, classified as ECCN 5A991, from the United States to Mayrow in Dubai, United Arab Emirates. The Mayrow case, set forth on page 25, 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 BIS's direction. Also, in December 2005, FedEx violated the EAR when it facilitated the unlicensed export of flight simulation software classified as ECCN 4A994 to Beijing University of Aeronautics and Astronautics (BUAA a/k/a Beihang University), an organization on the BIS Entity List located in China. 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 BIS'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 BIS'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.

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 reexport 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, BIS 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 the 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 BIS'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, CA 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 BIS'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 BIS'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 Italy and India. The technology was also controlled to India for nuclear nonproliferation reasons. This case resulted from an investigation conducted by BIS'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 BIS'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 persons on certain lists. 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 and 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 controls and deemed exports. The training modules are presented in a video streaming format.

In addition, Supplement No. 2 to 15 C.F.R. Part 766 provides guidance regarding BIS's penalty determination process in the settlement of administrative antiboycott of cases involving violations of Part 760 of the EAR, or violations of Part 762 (Recordkeeping) when the recordkeeping requirement pertains to Part 760. Similar to guidance regarding administrative export control cases, Supplement No. 2 to Part 766 describes how BIS determines appropriate penalties in settlement of violations in antiboycott cases. The guidance contains a comprehensive description of the factors taken into account in determining civil penalties including significant mitigating and aggravating factors.

As in export control cases, BIS encourages submission of Voluntary Self-Disclosures (VSDs) by parties who believe they may have violated the antiboycott provisions of the EAR. The procedures relating to antiboycott VSDs are set out in 15 C.F.R. 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.

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

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(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 nations 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

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).

Digi-Key Corporation

The Violation: During the years 2008 through 2011, in connection with transactions involving the sale and/or transfer of U.S. origin goods to Malaysia and the United Arab Emirates, Digi-Key Corporation (Digi-Key), located in Minnesota, on five occasions, furnished to its customer a statement that certain of the ordered goods were not made in Israel. Furnishing this information is prohibited because the information concerns Digikey's or another person's business relationships with or in a boycotted country. In addition, on fifty-eight occasions, Digi-Key received a goods directive prohibiting any import from Israel or of goods made in Israel. Digi-Key failed to report its receipts of these requests to engage in a restrictive trade practice or boycott. Digi-Key voluntarily disclosed these transactions to BIS.

The Penalty: On September 13, 2013, Digi-Key Corporation agreed to pay a civil penalty of $56,600.

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