Department of Justice

November 2019 NSD
WWW.JUSTICE.GOV (202) 514-2007

SUMMARY OF MAJOR U.S. EXPORT ENFORCEMENT, ECONOMIC ESPIONAGE, AND SANCTIONS-RELATED CRIMINAL CASES
(January 2016 to the present: updated November 2019)

Below are brief descriptions of some of the major export enforcement, economic espionage, and sanctions-related criminal prosecutions by the Department of Justice since January 2016. These cases resulted from investigations by the Federal Bureau of Investigation (FBI), Homeland Security Investigations (HSI), the Department of Commerce's Bureau of Industry and Security (BIS), the Pentagon's Defense Criminal Investigative Service (DCIS), and other law enforcement agencies. This list represents only select cases and is not exhaustive.

Cryptocurrency for North Korea – On Nov. 29, 2019, in the Southern District of New York, a criminal complaint was unsealed charging Virgil Griffith with violating the International Emergency Economic Powers Act (IEEPA) by traveling to the Democratic People's Republic of Korea ("DPRK" or "North Korea") in order deliver a presentation and technical advice on using cryptocurrency and blockchain technology to evade sanctions. Griffith, who is a citizen of the United States and a resident of Singapore, was arrested at Los Angeles International Airport on Nov. 28, 2019. According to the complaint unsealed in Manhattan federal court: Pursuant to the IEEPA and Executive Order 13466, U.S. persons are prohibited from exporting any goods, services, or technology to the DPRK without a license from Department of the Treasury, Office of Foreign Assets Control (OFAC). In or about April 2019, Griffith traveled to the DPRK to attend and present at the "Pyongyang Blockchain and Cryptocurrency Conference." Despite the Department of State denying Griffith permission to travel to the DPRK, Griffith presented at the Cryptocurrency Conference in the DPRK, knowing that doing so violated sanctions against the DPRK. At no time did Griffith obtain permission from OFAC to provide goods, services, or technology to the DPRK. At the Cryptocurrency Conference in the DPRK, Griffith and other attendees discussed how the DPRK could use blockchain and cryptocurrency technology to launder money and evade sanctions. After the Cryptocurrency Conference, Griffith began formulating plans to facilitate the exchange of cryptocurrency between North Korea and South Korea, despite knowing that assisting with such an exchange would violate sanctions against the DPRK. Griffith also encouraged other U.S. citizens to travel to North Korea and attend the DPRK Cryptocurrency Conference next year. This case is being investigated by the FBI and its New York Field Office.

Monsanto Trade Secrets – On Nov. 21, 2019, Haitao Xiang, 42, formerly of Chesterfield, Missouri, was indicted by a federal grand jury on one count of conspiracy to commit economic espionage, three counts of economic espionage, one count of conspiracy to commit theft of trade secrets, and three counts of theft of trade secrets. According to the indictment, Xiang was employed by Monsanto and its subsidiary, The Climate Corporation, from 2008 to 2017, where he worked as an imaging scientist. Monsanto and The Climate Corporation developed a digital, on-line farming software platform that was used by farmers to collect, store, and visualize critical agricultural field data and increase and improve agricultural productivity

for farmers. A critical component to the platform was a proprietary predictive algorithm referred to as the Nutrient Optimizer. Monsanto and The Climate Corporation considered the Nutrient Optimizer a valuable trade secret and their intellectual property. Haitao Xiang applied for, and ultimately was recruited into, the Chinese government's "Hundred Talents Program." In June 2017, the day after leaving employment with Monsanto and The Climate Corporation, Xiang bought a one-way plane ticket to China. Before he could board his flight, Xiang was intercepted at the airport by federal officials who seized copies of the Nutrient Optimizer. The FBI is investigating this case.

Military-Style Boats to China – On Nov. 1, 2019, in the Middle District of Florida, an indictment was returned charging four individuals – including two Chinese nationals, an active-duty U.S. Navy officer, and his wife – in a conspiracy to unlawfully smuggle military-style inflatable boats, with Evinrude MFE military outboard motors, to the People's Republic of China (PRC). The Navy officer and two other defendants also were charged with conspiring to violate firearms law, and the Navy officer has been charged with an additional firearms-related offense and with making false official statements. The four defendants charged in the indictment are: Fan Yang, 34, a naturalized citizen of the United States and Lieutenant in the U.S. Navy residing in Jacksonville, Florida; Yang Yang, 33, wife of Fan Yang, and a naturalized citizen of the United States residing in Jacksonville; Ge Songtao, 49, a citizen and resident of the PRC; and Zheng Yan, 27, a citizen and resident of the PRC. The defendants were arrested on Oct. 17, 2019. All four defendants have been charged with conspiring to submit false export information and to fraudulently attempt to export articles from the United States. Additionally, Yang Yang, Ge Songtao, and Zheng Yan have been charged with causing the submission of false and misleading information into the U.S. Automated Export System, and fraudulently attempting to export seven vessels and eight engines. Fan Yang, Yang Yang, and Ge Songtao are charged with other offenses as well – all three have been charged with conspiring to violate laws prohibiting an alien admitted under a nonimmigrant visa from possessing a firearm and prohibiting the transfer of a firearm to a nonresident. Fan Yang also was charged with making a false statement to a firearms dealer and making false official statements in his application for a security clearance. This case was investigated by the FBI; the U.S. Naval Criminal Investigative Service; the U.S. Department of Commerce, Bureau of Industry and Security; and the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives.

Scuba Equipment to Libya – On Oct. 29, 2019, Peter Sotis, 55, of Delray Beach, Florida, was arrested based on an indictment charging him with conspiracy to violate and attempted violation of the International Emergency Economic Powers Act (IEEPA) and the Export Administration Regulations (EAR), as well as smuggling of goods. The indictment alleges Sotis was the owner and principal of Add Helium, a Fort Lauderdale diving company. Sotis was charged with smuggling, conspiracy to violate and attempted violation of IEEPA and the EAR by transferring dual-use goods, that is, articles that have both civilian and military application, for export to Libya without the required Department of Commerce license. Court documents indicated that Sotis and a co-defendant at Add Helium transferred four rebreathers, which were controlled under the EAR for national security reasons, to a shipping company for export to Libya after being informed by a Commerce agent that the items could not be exported while a license determination was pending. A rebreather is an apparatus that absorbs the carbon dioxide of a scuba diver's exhaled breath to permit the rebreathing (recycling) of each breath. This technology produces no bubbles, thereby concealing the diver's activities from those on the surface, and allowing a diver to stay underwater longer compared with normal diving equipment. The investigation was conducted by Homeland Security Investigations and the Department of Commerce, with assistance from the FBI's Miami Field Office and U.S. Customs and Border Protection.

Industrial Equipment to Iran – On Oct. 24, 2019, an Ohio man was sentenced in U.S. District Court for exporting gas and oil pipeline parts to Iran for more than a decade in deliberate violation of a U.S. embargo and trade sanctions. Behrooz Behroozian, 64, of Columbus, was sentenced to 20 months in prison.

According to documents filed in this case: Behroozian was born in Iran and became a naturalized U.S. citizen in 1987. In November 2006, Behroozian became the owner and operator of a computer parts supplier in Dublin, Ohio, called Comtech International. Comtech had no storefront, made no domestic sales, and seldom exported computer parts. Instead, Comtech and Behroozian primarily exported industrial equipment to Sumar Industrial Equipment, in the United Arab Emirates, for further exportation to Iran. Behroozian used Sumar as an intermediary to attempt to cover-up that he was illegally supplying industrial equipment to Iran, in violation of the International Emergency Economic Powers Act (IEEPA). Behroozian exported manifolds, valves, and connectors used for industrial pipelines in the gas and oil refinement industry to Iran via Sumar and profited $35,000 to $40,000 per year. This violated embargo and trade sanctions imposed upon Iran by the United States in May 1995. The investigation was conducted by the FBI and the Department of Commerce.

North Korean Bulk Carrier Ship – On Oct. 21, 2019, the Department of Justice announced the entry of a judgment of forfeiture regarding the M/V Wise Honest (the "Wise Honest"), a 17,061-ton, single-hull bulk carrier ship registered in the Democratic People's Republic of Korea ("DPRK" or "North Korea"). The judgment of forfeiture, which was ordered by the Honorable P. Kevin Castel of the Southern District of New York, confirms the U.S. Government's ownership of the Wise Honest. The Wise Honest, one of the DPRK's largest bulk carriers, was used to illicitly ship coal from North Korea and to deliver heavy machinery back to North Korea. Payments for maintenance, equipment, and improvements of the Wise Honest were made in U.S. dollars through unwitting U.S. banks. This conduct violated longstanding U.S. law and United Nations Security Council resolutions. According to documents filed in Manhattan federal court: Pursuant to the International Emergency Economic Powers Act (IEEPA) and the North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA), the DPRK and individuals or entities that the Department of the Treasury, Office of Foreign Assets Control (OFAC) has determined are involved in the facilitation of proliferation of weapons of mass destruction (WMDs) are prohibited from engaging in transactions with U.S. persons, involving U.S.-origin goods, or using the U.S. financial system. The United Nations Security Council has similarly prohibited the provision of goods, technology, and services to North Korea, and the sale, supply, or transfer of coal from North Korea. On May 9, 2019, the U.S. Attorney's Office filed a civil forfeiture complaint against the Wise Honest, which had previously been seized pursuant to a warrant issued in the Southern District of New York. The case was investigated by the FBI and its New York Field Office, Counterintelligence Division, with assistance from the Department of Justice's Money Laundering and Asset Recovery Section and Office of International Affairs; the U.S. Coast Guard; and the U.S. Department of State.

Military-Grade Technology to China – On Oct. 16, 2019, Tao Li, a 39-year-old Chinese national, was sentenced to 40 months in prison, followed by three years of supervised release. Li previously had pleaded guilty to conspiring to export military- and space-grade technology to the People's Republic of China (PRC) without a license, in violation of the International Emergency Economic Powers Act. Between December 2016 and January 2018, Li worked with other individuals in China to purchase radiation-hardened power amplifiers and supervisory circuits and illegally export them from the United States to China. The electronic components sought by Li are capable of withstanding significant levels of radiation and extreme heat, and as a result, are primarily used for military and space applications. Due to the technological capabilities of the electronic components sought by Li and the significant contribution that the components could make to a foreign country's military and space programs, both parts required an export license from the U.S. Department of Commerce, Bureau of Industry and Security, prior to being sent out of the United States. Notwithstanding the licensing requirement, the Department of Commerce has a policy of denial to export these types of electronic components to the PRC. Li, who resided in China, used multiple aliases to contact individuals in the United States, including representatives of United States-based private companies, to try to obtain the electronic components. Additionally, Li and his co-conspirators agreed to pay a "risk fee" to illegally export the electronic components to China. In furtherance of his request, Li wired money from a

bank account in China to a bank account in Arizona. Li was arrested in September 2018 at Los Angeles International Airport, as Li attempted to travel from China to Arizona. The investigation in this case was conducted by HSI and DCIS.

Iranian Sanctions Evasion Scheme – On Oct. 15, 2019, the Department of Justice announced that TÜRKİYE HALK BANKASI A.S., a/k/a "Halkbank," was charged in a six-count indictment with fraud, money laundering, and sanctions offenses related to the bank's participation in a multibillion-dollar scheme to evade U.S. sanctions on Iran. According to allegations in the indictment, returned in Manhattan federal court: From approximately 2012 to 2016, Halkbank was a foreign financial institution organized under the laws of and headquartered in Turkey. The majority of Halkbank's shares are owned by the Government of Turkey. Halkbank and its officers, agents, and co-conspirators directly and indirectly used money service businesses and front companies in Iran, Turkey, the United Arab Emirates, and elsewhere to violate and evade prohibitions against Iran's access to the U.S. financial system, restrictions on the use of proceeds of Iranian oil and gas sales, and restrictions on the supply of gold to the Government of Iran and to Iranian entities and persons. Halkbank knowingly facilitated the scheme, participated in the design of fraudulent transactions intended to deceive U.S. regulators and foreign banks, and lied to U.S. regulators about Halkbank's involvement. Halkbank was charged with (1) conspiracy to defraud the United States, (2) conspiracy to violate the International Emergency Economic Powers Act (IEEPA), (3) bank fraud, (4) conspiracy to commit bank fraud, (5) money laundering, and (6) conspiracy to commit money laundering. The Department of Justice previously charged nine individual defendants, including bank employees, the former Turkish Minister of the Economy, and other participants in the scheme. The investigation was conducted by the FBI.

U.S. Aviation Trade Secrets – On Sep. 11, 2019, in the Southern District of Ohio, a federal grand jury indicted two defendants and charged them with conspiring and attempting to steal trade secrets from an American aviation company. Italian national Maurizio Paolo Bianchi, 59, and Russian national Alexander Yuryevich Korshunov, 57, had been charged by a criminal complaint on Aug. 21. Korshunov was arrested on Aug. 30 at Naples International Airport in Italy. Bianchi was arrested on Oct. 2 in Marino, Italy, pursuant to a provisional arrest request from the United States. According to the indictment, Korshunov was an employee of a Russian state-owned company and had previously been a Russian public official whose service included the Ministry of Foreign Affairs. Bianchi was a former director at Avio S.p.A, an Italian aerospace company, until 2012. GE Aviation purchased the aerospace business from Avio S.p.A. in 2013 and operates the business as Avio Aero with its headquarters in Turin, Italy. GE Aviation is one of the world's top aircraft engine suppliers and is headquartered in the Southern District of Ohio. After leaving Avio S.p.A, Bianchi went to work for a company called Aernova in Forli, Italy. Korshunov was employed at United Engine Corp (UEC), which included a subsidiary named Aviadvigatel (a branch of the Russian state-owned company), which had been "entity listed" by the U.S. Department of Commerce in September 2018 for acting contrary to the national security or foreign policy interests of the United States. Aernova and Aviadvigatel had a contract during the time of the alleged conduct. It is alleged that between 2013 and 2018, Bianchi – on behalf of Korshunov – recruited current or former employees of Avio Aero to do consulting work related to jet engine accessory gearboxes. An accessory gearbox is a component mechanism used to transfer the power from the jet engine to other airplane power systems. According to court documents, the employees' statements of work typically stated that the "the holders of patent and intellectual property obtained as a result of the work are … the Ministry of Industry and Trade of the Russian Federation." Employees allegedly used trade secrets owned by Avio Aero and GE Aviation to create a technical report. The effort focused on accessory gearboxes made by Avio Aero that provide power to systems such as hydraulic pumps, generators, and fuel pumps. Court documents detail that Korshunov allegedly arranged and paid for employees to meet with him, in June 2013 at the Paris Air Show in France and in 2014 in Italy, to discuss and revise the technical report. The investigation was conducted by the FBI.

Arms Export Control Act Violations – On Sep. 4, 2019, in the District of New Jersey, the owner of two defense contracting firms was sentenced to 36 months in prison for providing non-conforming parts for military equipment, illegally sharing sensitive technical information, and evading income taxes. Roger Sobrado, 49, of Marlton, New Jersey, previously pleaded guilty before U.S. District Judge Noel L. Hillman to an information charging him with one count each of conspiracy to commit wire fraud, conspiracy to violate the Arms Export Control Act, and income tax evasion. In addition to the prison term, Judge Hillman sentenced Sobrado to three years of supervised release and ordered him to pay $8,043,977 in restitution. According to documents filed in this case and statements made in court: Sobrado was the owner of two companies: Tico Manufacturing Inc. (TICO), a purported manufacturing company, and Military and Commercial Spares Inc. (MCS), a defense contracting company, both in Berlin Township, New Jersey. Sobrado admitted that between January 2011 and December 2015, MCS obtained contracts with the U.S. Department of Defense (DoD) by falsely claiming that the military parts it contracted to provide would be exactly as described and provided by authorized manufacturers. The DoD contracts specified that the parts were critical application items for military equipment, including fighter jets and helicopters. Sobrado recruited various family members to participate in the scheme by establishing companies that contracted with the DoD. Those companies also obtained contracts with the DoD by falsely claiming that the military parts they contracted to provide would be the exact product described and would be provided by authorized manufacturers. In fact, Sobrado used TICO to contract with local manufacturers to supply non-conforming parts to MCS and his family members' companies at a significantly reduced cost. The non-conforming parts supplied by Sobrado were shipped from New Jersey to various DoD locations around the country. Sobrado also admitted that in August 2005 and in November 2010 he submitted to the DoD a fraudulent application for access to export controlled drawings and technical data on behalf of a family member's company. Sobrado acknowledged that access to the controlled drawings and technical data was limited to citizens of the United States and to those lawfully in the United States. Sobrado said he submitted the application because his family member told him that he needed access to drawings and that he could not get them because he was not a U.S. citizen. Sobrado agreed that in July 2011, and at various times between January 2013 and November 2015, the family member, who is illegally in the United States, accessed or downloaded hundreds of drawings that were sensitive in nature and that required special access. The case was investigated by the Department of Defense, Defense Criminal Investigative Service Northeast Field Office; the Department of Homeland Security, Homeland Security Investigations; IRS - Criminal Investigation; the Social Security Administration, Office of Inspector General; and the U.S. Attorney's Office.

Carbon Fiber to Iran – On Aug. 29, 2019, Behzad Pourghannad pleaded guilty to participating in a conspiracy to export carbon fiber from the United States to Iran between 2008 and 2013. Pourghannad, 65, who is an Iranian citizen, pled guilty to one count of conspiracy to violate the International Emergency Economic Powers Act. On Nov. 13, 2019, he was sentenced to 46 months in prison. According to the indictment and statements made at Pourghannad's guilty plea: Between 2008 and July 2013, Pourghannad and his two co-defendants, Ali Reza Shokri and Farzin Faridmanesh, lived in Iran and worked together to obtain carbon fiber from the United States and surreptitiously export it to Iran via third countries. Shokri and Faridmanesh remain at liberty. In particular, Shokri worked to procure many tons of carbon fiber from the United States; Pourghannad agreed to serve as the financial guarantor for large carbon fiber transactions; and Faridmanesh agreed to serve as the trans-shipper. Carbon fiber has a wide variety of uses, including in missiles, aerospace engineering, and gas centrifuges that enrich uranium No one involved in these transactions obtained permission from the U.S. Department of Treasury, Office of Foreign Assets Control, to export the carbon fiber from the United States. The investigation was conducted by the FBI and the Department of Commerce, with assistance from the U.S. Marshals Service, Homeland Security Investigations, and Immigration and Customs Enforcement.

Anti-Aircraft Missiles Scheme – On Aug. 20, 2019, a black-market arms dealer with a long history of brokering machine guns, rocket-propelled grenades, and anti-tank armaments – and who was found guilty

in a scheme to sell and use surface-to-air missiles – was sentenced to 30 years in federal prison. Rami Najm Asad-Ghanem, 53, who was commonly known as Rami Ghanem, a naturalized United States citizen who was living in Egypt at the time of the offenses, was sentenced by U.S. District Judge S. James Otero. Following a nine-day trial in November 2018, a federal jury found Ghanem guilty of conspiring to use and to transfer missile systems designed to destroy aircraft. The day before his trial started, Ghanem pleaded guilty to six other federal crimes stemming from his arms-trafficking activities, including the unlicensed export of weapons and ammunition, smuggling, money laundering, and unlicensed arms brokering. The evidence presented at trial showed that Ghanem conspired to transfer a wide array of surface-to-air missile systems to customers around the world, including clients in Libya, the United Arab Emirates, Iraq, and the leadership of Hezbollah, a designated foreign terrorist organization. During the trial, prosecutors showed that he conspired to use Russian-made Igla and Strela surface-to-air missile systems by brokering the services of mercenary missile operators to a militant faction in Libya in 2015. Among other actions, Ghanem negotiated the salaries and terms of service of the mercenary missile operators, coordinated their payment, facilitated their travel to Libya, confirmed their arrival and performance of duties, and offered them a $50,000 bonus if they were successful in their mission of shooting down airplanes flown by the internationally recognized government of Libya. In addition to numerous documents that demonstrated Ghanem's role in the conspiracy, the jury viewed videos of sworn deposition testimony of two missile operators and Ghanem's fellow arms broker who assisted in procuring their services for this transaction. In documents filed in relation to sentencing, prosecutors offered evidence of a contract documenting Ghanem's agreement to sell $250 million worth of weapons and ammunition to a militant faction in Libya; a contract between Ghanem and the Egyptian Ministry of Defense dealing with hundreds of rocket-propelled grenade launchers; attempts to buy and sell combat jets and helicopter gunships; and his apparent role in the trafficking of counterfeit currency, looted antiquities, and black-market diamonds. Ghanem was arrested on Dec. 8, 2015, in Athens, Greece. He was extradited to the United States in April 2016 to face prosecution in this case, and has remained in custody without bond since the time of his arrest. The investigation was led by U.S. Immigration and Customs Enforcement's Homeland Security Investigations, which received substantial assistance from the Department of Defense's Criminal Investigative Service; the Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; U.S. Customs and Border Protection; and the Hellenic National Police.

Manufacturing Equipment to Iran – On Aug. 18, 2019, in the Central District of California, federal authorities arrested a resident of Iran who was charged in a scheme to ship prohibited items from the United States to Iran, in violation of the International Emergency Economic Powers Act (IEEPA) and U.S. sanctions imposed on Iran. Mehdi Hashemi, who sometimes used the name "Eddie Hashemi," 46, a dual citizen of the United States and Iran who previously resided in Los Angeles, was charged in a 21-count indictment that was unsealed on Aug. 19. The indictment charges Hashemi with conspiring to violate IEEPA, violating IEEPA, smuggling, money laundering, unlawful export information activities, and making false statements. Hashemi allegedly participated in a conspiracy to illegally export to Iran computer numerical control (CNC) machines, which are used to process raw materials, such as metals, to precise standards. The CNC machines at issue in this case are export-controlled for nuclear non-proliferation and anti-terrorism reasons. After being taken into custody after arriving at Los Angeles International Airport on a flight from Turkey, Hashemi was arraigned on the indictment. He entered not guilty pleas and was ordered held without bond. The indictment outlines a scheme in which Hashemi purchased CNC machines and related equipment from suppliers in the United States and Canada, made arrangements to ship the machines to the United Arab Emirates (UAE) under false and forged invoices and packing lists, and then arranged to forward the machines from the UAE to Iran. Hashemi purchased the machines on behalf of a Tehran-based company identified in the indictment as "Company A," an outfit that claimed to manufacture textiles, medical and automotive components, and spare parts. Hashemi also is charged with making false statements to federal authorities in 2018 when he lied about his activities, his knowledge of federal export laws, and his intention to send the CNC machines to Iran. A second defendant charged in the indictment – Feroz

Khan, of the United Arab Emirates, who allegedly helped to ship CNC machines from the UAE to Iran – is a fugitive. The case is being investigated by the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement, which received significant assistance from U.S. Immigration and Customs Enforcement's Homeland Security Investigations and U.S. Customs and Border Protection.

Turbine Parts to Iran – On July 19, 2019, in the Northern District of New York, Mahin Mojtahedzadeh (Mahin), age 74, a citizen of Iran, pleaded guilty to conspiring to unlawfully export gas turbine parts from the United States to Iran. Mahin pleaded guilty to one count of conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations. She admitted that she was the President and Managing Director of ETCO-FZC (ETCO), an export company with an office in Dubai in the United Arab Emirates. ETCO is a supplier of spare and replacement turbine parts for power generation companies in the Middle East, including Iran. Mahin admitted that from 2013 through 2017, she worked with companies in Canada and Germany to violate and evade U.S. sanctions against Iran, by having these companies first acquire more than $3 million dollars' worth of turbine parts from two distributors in Saratoga County, New York. When the U.S. parts arrived in Canada and Germany, respectively, these companies and Mahin then arranged for the parts to be re-shipped to ETCO's customers in Iran. At all times, U.S. law prohibited the export and re-export of U.S.-origin turbine parts to Iran without a license from the Treasury Department's Office of Foreign Assets Control (OFAC), which neither Mahin nor her co-conspirators possessed. Two of Mahin's co-conspirators previously pleaded guilty. Olaf Tepper, age 52, and a citizen of Germany, pleaded guilty to conspiring to violate IEEPA. On Aug. 3, 2018, he was sentenced to 24 months in prison, and to pay a $5,000 fine. Tepper was the Founder and Managing Director of Energy Republic GmbH (Energy Republic), based in Cologne, Germany, which re-exported U.S.-origin turbine parts to Iran, as part of a conspiracy with Mahin. Mojtaba Biria, age 68, and a citizen of Germany, also pleaded guilty to conspiring to violate IEEPA, and was sentenced to time served (about 21 months in jail) and fined $5,000. Biria was Energy Republic's Technical Managing Director. These cases are the result of a joint investigation by the FBI, HSI, and BIS.

Aircraft Parts and Services to Iran – On June 4, 2019, in U.S. District Court for the District of Columbia, two separate indictments were unsealed charging Peyman Amiri Larijani, 33, a citizen of Iran and former resident of Istanbul, Turkey. On April 22, 2015, a 34-count indictment was returned charging Larijani and a Turkish based company, Kral Havacilik IC VE DIS Ticaret Sirketi (Kral Aviation), with conspiracy to acquire U.S. origin aircraft parts and goods to supply to entities and end-users in Iran, to conceal from United States companies and the U.S. government that the U.S.-origin goods were destined for Iranian aviation business end users, to make financial profit for defendants and other conspirators, and to evade the regulations, prohibitions, and licensing requirements of the International Emergency Economic Powers Act (IEEPA), the Iranian Transactions and Sanctions Regulations (ITSR), and the Export Administration Regulations (EAR). According to this indictment, beginning around December 2010 through July 2012, Larijani was the Operations Manager for Kral Aviation. Larijani and his co-conspirators purchased U.S.-origin aircraft parts and accessories from U.S. companies. Larijani and his co-conspirators wired money to banks in the United States as payment for these parts and concealed from U.S. sellers the ultimate end use and end users of the purchased parts. Larijani and his co-conspirators caused these parts to be exported from the United States to Turkey, before shipping to airlines in Iran including Mahan Air, Sahand Air, and Kish Air. Mahan Air has been designated by the U.S. Department of the Treasury as a Specially Designated National (SDN) for providing financial, material, and technological support to Iran's Islamic Revolutionary Guard Corps-Qods Force. The Department of Commerce has placed Mahan on its Denied Parties List and Kral Aviation on the Entity List. On Oct. 6, 2016, a four-count indictment was returned charging Larijani along with Mahan Air, Kral Aviation, Toufan Amiri Larijani, Javad Rajabi, Mehdi Bahrami, and Ghodratollah Zarei with conspiracy to export U.S. goods to Iran, specifically U.S. origin commercial aircraft engines, and provide services to a Mahan Air, an SDN, and to defraud the United States; unlawful exports and attempted exports to embargoed country and provision of services to an SDN; willful violation

of denial order; and conspiracy to commit money laundering for purchasing a U.S. origin aircraft engine to supply to Mahan Air in Iran without obtaining an export license. According to this indictment, beginning around April 2012 through September 2012, Larijani and his co-conspirators attempted to acquire U.S. origin aircraft engines to supply to Mahan Air in Iran without obtaining a license or other authorization from the United States. Larijani and his co-conspirators caused the shipment of an aircraft engine from the United States with the express purpose of re-exporting the aircraft engine to Iran. Investigation was conducted by special agents from the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement.

General Electric Trade Secrets – On April 23, 2019, an indictment was unsealed charging Xiaoqing Zheng, 56, of Niskayuna, New York, and Zhaoxi Zhang, 47, of Liaoning Province, China, with economic espionage and conspiring to steal General Electric (GE) trade secrets regarding turbine technologies, knowing and intending that those stolen trade secrets would be used to benefit the People's Republic of China (PRC). According to the 14-count indictment, Zheng, while employed at GE Power & Water in Schenectady, New York as an engineer specializing in sealing technology, exploited his access to GE's files by stealing multiple electronic files, including proprietary files involving design models, engineering drawings, configuration files, and material specifications having to do with various components and testing systems associated with GE gas and steam turbines. Zheng emailed and transferred many of the stolen GE files to his business partner, Chinese businessman Zhaoxi Zhang, who was located in China. Zheng and Zhang used the stolen GE trade secrets to advance their own business interests in two Chinese companies – Liaoning Tianyi Aviation Technology Co., Ltd. (LTAT) and Nanjing Tianyi Avi Tech Co. Ltd. (NTAT), companies which research, develop, and manufacture parts for turbines. The indictment also alleges that Zheng and Zhang conspired to commit economic espionage, as the thefts of GE's trade secrets surrounding various turbine technologies were done knowing and intending that the thefts would benefit the PRC and one or more foreign instrumentalities, including LTAT, NTAT, Shenyang Aerospace University, Shenyang Aeroengine Research Institute, and Huaihai Institute of Technology. The defendants, through LTAT and NTAT, received financial and other support from the Chinese government and coordinated with Chinese government officials to enter into research agreements with Chinese state-owned institutions to develop turbine technologies. Zheng was arraigned in Albany, New York, before U.S. Magistrate Judge Christian F. Hummel, and released with conditions pending trial. This case is being investigated by the Federal Bureau of Investigation.

Financial Transactions for Iranian Entities – On April 15, 2019, UniCredit Bank AG (UCB AG), a financial institution headquartered in Munich, Germany, operating under the name HypoVereinsbank, and part of the UniCredit Group agreed to enter a guilty plea to conspiring to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States by processing hundreds of millions of dollars of transactions through the U.S. financial system on behalf of an entity designated as a weapons of mass destruction proliferator and other Iranian entities subject to U.S. economic sanctions. UniCredit Bank Austria (BA), another financial institution in the UniCredit Group, headquartered in Vienna, Austria, agreed to forfeit $20 million and entered into a non-prosecution agreement to resolve an investigation into its violations of IEEPA. UniCredit SpA, the parent of both UCB AG and BA, has agreed to ensure that UCB AG and BA's obligations are fulfilled. UCB AG will waive indictment and plead guilty to a one-count felony criminal information, charging UCB AG with knowingly and willfully conspiring to commit violations of IEEPA and to defraud the United States, from 2002 through 2011. UCB AG has entered into a written plea agreement, has accepted responsibility for its criminal conduct, and will enter its guilty plea before a judge in the District of Columbia. UniCredit Group banks will pay total financial penalties of approximately $1.3 billion. The plea agreement, subject to approval by the court, provides that UCB AG will forfeit $316,545,816 and pay a fine of $468,350,000. In addition, UCB AG has entered into a plea agreement with the New York County District Attorney's Office (DANY) for violating New York State law pursuant to which it will pay $316,545,816. BA also has entered into a non-prosecution agreement

with DANY for violating New York State law. UniCredit SpA, UCB AG, and BA also have entered into various settlement agreements with the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the Board of Governors of the Federal Reserve System, and the New York State Department of Financial Services (DFS) under which they will pay additional penalties of approximately $660 million as follows: $611,023,421 to OFAC, which will be satisfied in part by payments to the Justice Department and the Federal Reserve, $157,770,000 to the Federal Reserve, and $405 million to DFS. The case was investigated by the FBI, IRS-Criminal Investigations, and DANY.

Bank Transactions for Iran – On April 9, 2019, the Justice Department announced that Standard Chartered Bank (SCB), a global financial institution headquartered in London, England, agreed to forfeiture of $240 million, a fine of $480 million, and to the amendment and extension of its deferred prosecution agreement (DPA) with the Justice Department for an additional two years for conspiring to violate the International Emergency Economic Powers Act (IEEPA). This criminal conspiracy, lasting from 2007 through 2011, resulted in SCB processing approximately 9,500 financial transactions worth approximately $240 million through U.S. financial institutions for the benefit of Iranian entities. The New York County District Attorney's Office (DANY) also announced that SCB has agreed to amend its DPA with DANY and extend for two additional years, and to pay an additional financial penalty of $292,210,160. Under the amended DPA with DANY, SCB admitted that it violated New York State law by, among other things, falsifying the records of New York financial institutions. SCB also entered into separate settlement agreements with the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the Board of Governors of the Federal Reserve System, the New York State Department of Financial Services, and the United Kingdom's Financial Conduct Authority under which SCB shall pay additional penalties totaling more than $477 million. The Justice Department has agreed to credit a portion of these related payments and, after crediting, will collect $52,210,160 of the fine, in addition to SCB's $240 million forfeiture. In connection with the conspiracy, a former employee of SCB's branch in Dubai, United Arab Emirates (UAE), referred to as Person A, pleaded guilty in the District of Columbia for conspiring to defraud the United States and to violate IEEPA. A two-count criminal indictment also was unsealed in federal court in the District of Columbia charging Mahmoud Reza Elyassi, an Iranian national, 49, and former customer of SCB Dubai, with participating in the conspiracy. As part of the amended DPA, SCB admitted that, from 2007 through 2011, two former employees of its branch in Dubai willfully conspired to help Iran-connected customers conduct U.S. dollar transactions through the U.S. financial system for the benefit of Iranian individuals and entities. One of these Iran-connected customers was Elyassi, an Iranian national who operated business accounts with SCB's Dubai branch while residing in Iran. SCB's former employees helped Elyassi manage these accounts, concealed their Iranian connections, and facilitated foreign currency transactions in U.S. dollars.

Aircraft Parts to Iran – On March 21, 2019, in the District of Columbia, an Australian man was sentenced to 24 months in prison on four counts of violations of the International Emergency Economic Powers Act, which criminalizes knowing transactions with Iranian entities without a license from the U.S. Treasury Department. David Russell Levick, 57, of Cherrybrook NSW, Australia, pleaded guilty to the charges on Feb. 1, 2019, in U.S. District Court. He was sentenced by the Honorable James E. Boasberg. In addition to the prison term, Levick must pay a forfeiture amount of $199,227, which represents the total value of the goods involved in the illegal transactions. Following completion of his prison term, Levick will be subject to deportation proceedings. According to the plea documents, Levick was the general manager of ICM Components, Inc., located in Thornleigh, Australia. He solicited purchase orders and business for the goods from a representative of a trading company in Iran. This person in Iran, referenced in court documents as "Iranian A," also operated and controlled companies in Malaysia that acted as intermediaries for the Iranian trading company. Levick then placed orders with U.S. companies on behalf of "Iranian A" for the goods, which were aircraft parts and other items that "Iranian A" could not have directly purchased from the United States without the permission of the U.S. government. The defendant admitted to procuring or attempting

to procure U.S. items for transshipment to Iran, each of which required a license from the Treasury Department prior to any export. The activities took place in 2007 and 2008. Levick was indicted in February 2012. At the request of the United States, Australia arrested him for the purposes of extradition, and Australia extradited him to the United States in December 2018. The investigation was conducted by agents from the FBI's Washington Field Office, the Department of Commerce's Bureau of Industry and Security, and the Boston Office of the Immigration and Customs Enforcement.

Electronic Components to Russia – On March 20, 2019, a 52-count indictment was unsealed charging Valery Kosmachov with engineering a scheme to illegally procure sophisticated electronic components from the United States and to smuggle them into the Russian Federation. According to the indictment, filed on Sep. 21, 2017, Kosmachov, 66, is an Estonian national and resident of Tallinn, Estonia. He served as owner of Adimir OU and co-owner of Eastline Technology OU, along with co-defendant and Russian national Sergey Vetrov, 66. Kosmachov, Vetrov, and their two companies are charged with conspiracy, violating the International Emergency Economic Powers Act (IEEPA), smuggling, and international money laundering. The indictment describes how Kosmachov and Vetrov used the Estonia-based companies as procurement "fronts" to obtain controlled U.S.-origin microelectronics, in part by misrepresenting that the end-users for the components were located in Estonia. The components included dual-use programmable computer chips capable of operating in austere environments, making them useful in both civilian and military applications. Once in possession of the chips in Estonia, the co-defendants allegedly later smuggled them into the Russian Federation, in part by using laundered funds. Kosmachov was arrested in Tallinn on Sep. 12, 2018, and was extradited to the United States on March 14, 2019, to face prosecution. Vetrov remains at large. The prosecution is the result of an investigation by Homeland Security Investigations, the Department of Commerce's Bureau of Industry and Security, U.S. Customs and Border Protection, the Internal Revenue Service, and the U.S. Marshals Service, with assistance from the Department of Justice's Office of International Affairs.

Firearms to Hong Kong – On Jan. 31, 2019, in the District of Massachusetts, two Malaysian nationals were arrested and charged with conspiring to illegally export firearms and firearm parts from the United States to an individual located in Hong Kong, China. Lionel Chan, 35, who resided in Brighton, Mass., and Muhammad Radzi, 26, who resided in Brooklyn, N.Y., were charged by criminal complaint with one count of conspiring to violate the Arms Export Control Act. Chan also was charged with one count of obstruction of justice. According to the criminal complaint, beginning in or around March 2018, Chan began purchasing a variety of U.S.-origin firearm parts, including parts used to assemble AR-15 assault rifles and 9MM semi-automatic handguns, at the request of a buyer in Hong Kong. Chan purchased the parts online through a variety of websites, including eBay and gunbroker.com. These firearm parts are restricted items and cannot be exported from the United States without a license. Nevertheless, Chan allegedly shipped the firearm parts via Federal Express to the buyer in Hong Kong without first obtaining the necessary export licenses. Chan intentionally concealed the contents of the shipments by providing false descriptions of the items contained in each shipment and by concealing the parts inside the package. Between March and May 2018, Chan shipped 12 packages from Brighton, Mass., to the buyer in Hong Kong. In or around April 2018, Radzi allegedly joined the conspiracy and began illegally exporting firearm parts to Hong Kong as well. Between May and October 2018, Radzi allegedly shipped 21 packages from Brooklyn, N.Y., to the buyer in Hong Kong. In October 2018, two of those packages were interdicted by Hong Kong authorities and found to contain numerous firearms parts, including a firing pin and gun sight, which were export-controlled. Like Chan, Radzi failed to obtain an export license for any of these shipments. The case is being investigated by Homeland Security Investigations in Boston. The Massachusetts State Police and U.S. Customs and Border Protection also assisted in the investigation.

Chinese Telecom Business in Iran – On Jan. 28, 2019, in the Eastern District of New York, a 13-count indictment was unsealed in federal court in Brooklyn charging four defendants, including Huawei

Technologies Co. Ltd. (Huawei), the world's largest telecommunications equipment manufacturer, with headquarters in the People's Republic of China (PRC) and operations around the world. The indicted defendants include Huawei and two Huawei affiliates – Huawei Device USA Inc. (Huawei USA) and Skycom Tech Co. Ltd. (Skycom) – as well as Huawei's Chief Financial Officer (CFO) Wanzhou "Cathy" Meng (Meng). Defendants Huawei and Skycom are charged with bank fraud and conspiracy to commit bank fraud, wire fraud and conspiracy to commit wire fraud, violations of the International Emergency Economic Powers Act (IEEPA) and conspiracy to violate IEEPA, and conspiracy to commit money laundering. Huawei and Huawei USA are charged with conspiracy to obstruct justice related to the grand jury investigation in the Eastern District of New York. Meng is charged with bank fraud, wire fraud, and conspiracies to commit bank and wire fraud. The charges in this case relate to a long-running scheme by Huawei, its CFO, and other employees to deceive numerous global financial institutions and the U.S. government regarding Huawei's business activities in Iran. As alleged in the indictment, beginning in 2007, Huawei employees lied about Huawei's relationship to a company in Iran called Skycom, falsely asserting it was not an affiliate of Huawei. The company further claimed that Huawei had only limited operations in Iran and that Huawei did not violate U.S. or other laws or regulations related to Iran. Most significantly, after news publications in late 2012 and 2013 disclosed that Huawei operated Skycom as an unofficial affiliate in Iran and that Meng had served on the board of directors of Skycom, Huawei employees, and in particular Meng, continued to lie to Huawei's banking partners about Huawei's relationship with Skycom. They falsely claimed that Huawei had sold its interest in Skycom to an unrelated third party in 2007 and that Skycom was merely Huawei's local business partner in Iran. In reality, Skycom was Huawei's longstanding Iranian affiliate, and Huawei orchestrated the 2007 sale to appear as an arm's length transaction between two unrelated parties, when in fact Huawei actually controlled the company that purchased Skycom. According to the indictment: Huawei relied on its global banking relationships for banking services that included processing U.S.-dollar transactions through the United States. U.S. laws and regulations generally prohibited these banks from processing transactions related to Iran through the United States. The banks could have faced civil or criminal penalties for processing transactions that violated U.S. laws or regulations. Relying on the repeated misrepresentations by Huawei, these banks continued their banking relationships with Huawei. One bank cleared more than $100 million worth of Skycom-related transactions through the United States between 2010 and 2014. In furtherance of this scheme to defraud, Huawei and its principals repeatedly lied to U.S. government authorities about Huawei's business in Iran in submissions to the U.S. government, and in responses to government inquiries. In 2017, when Huawei became aware of the government's investigation, Huawei and its subsidiary Huawei USA allegedly tried to obstruct the investigation by making efforts to move witnesses with knowledge about Huawei's Iran-based business to the PRC, and beyond the jurisdiction of the U.S. government, and by concealing and destroying evidence of Huawei's Iran-based business. In December 2018, Canadian authorities apprehended Meng in Vancouver pursuant to a provisional arrest warrant issued under Canadian law. The U.S. government is seeking Meng's extradition to the United States. The investigation is being jointly conducted by the FBI's New York Field Office, HSI's New York Field Office, OEE's New York Field Office, and DCIS's Southwest and Northeast Field Offices.

Firearms to Lebanon – On Nov. 8, 2018, in the Western District of Washington, Hicham Diab, of Tripoli, Lebanon and Nafez El Mir, a Canadian citizen residing in Lebanon, were arrested after they traveled to a Seattle warehouse and began hiding firearms in a vehicle they planned to ship to Lebanon. Diab and El Mir appeared in federal court on Nov. 9, 2018, charged with conspiracy to violate the Arms Export Control Act (AECA). Both men were detained pending additional hearings. According to a criminal complaint, in 2016 Diab began communicating with a person in the U.S. who Diab believed was willing to locate firearms for him to smuggle to Lebanon. The person in the U.S. alerted Homeland Security Investigations (HSI) about the contact. Over the course of 2017 and 2018, undercover HSI agents posed as people able and willing to supply firearms sought by Diab in furtherance of his smuggling scheme. In October 2018, Diab made plans to come to the U.S. and successfully wired funds for the purchase of firearms and a vehicle in which to hide

the firearms. Diab arrived in Seattle on November 7, 2018, and was accompanied by El Mir who, according to Diab, had experience smuggling firearms hidden in automobile panels. On November 7 and 8, Diab went with the undercover agents to a warehouse containing firearms that had been secured by HSI and the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), and inspected the firearms, which included: twenty Glock handguns, a Smith & Wesson .50 revolver, one FN Fiveseven pistol, an AR15 rifle kit and a M203 grenade launcher. Diab and El Mir, during their November 8 warehouse visit, began hiding the firearms in door panels and bumper space inside a sport-utility vehicle. El Mir also discussed ways to get the vehicle shipped to Lebanon with the hidden weapons. The men were arrested the evening of November 8 as they exited the warehouse. Diab and El Mir each pleaded guilty to conspiracy to violate the AECA, and being an alien in possession of a firearm. On June 11, 2019, Diab and El Mir each was sentenced to 18 months in prison. The case was investigated by HSI and ATF.

Controlled Technology to Iran – On Nov. 7, 2018, Arash Sepehri, 38, a citizen of Iran, pleaded guilty to a federal charge stemming from his role in a conspiracy to cause the export of controlled goods and technology to Iran, in violation of U.S. Department of Commerce and military controls, as well as in contravention of sanctions imposed against Iran. Sepehri pleaded guilty, in the U.S. District Court for the District of Columbia, to conspiracy to unlawfully export U.S. goods to Iran in violation of the International Emergency Economic Powers Act and the Iranian Transactions and Sanctions Regulations, and to defraud the United States. According to court documents filed in this case, Sepehri was an employee and a member of the board of directors of an Iranian company, Tajhiz Sanat Shayan, or Tajhiz Sanat Company (TSS). TSS and other companies involved in the conspiracy were listed by the European Union on May 23, 2011, as entities being sanctioned for their involvement in the procurement of components for the Iranian nuclear program. Through TSS and associated companies, Sepehri and others conspired to obtain high-resolution sonar equipment, data input boards, rugged laptops, acoustic transducers, and other controlled technology from the United States without obtaining proper licenses and in violation of economic sanctions. As stated in the court documents, Sepehri and his co-conspirators sought to evade legal controls through a variety of means, including the use of a variety of aliases, United Arab Emirates (UAE)-based front companies and an intermediary shipping company based in Hong Kong. Payments for the goods were arranged through the UAE. On March 21, 2019, Sepehri was sentenced to 25 months in prison (with credit for time served) followed by deportation proceedings. This investigation was conducted jointly by agents from FBI's Washington Field Office and HSI Washington, D.C.

Semiconductor Trade Secrets to PRC – On Nov. 1, 2018, in the Northern District of California, an indictment was unsealed charging a state-owned enterprise of the People's Republic of China (PRC), a Taiwan company, and three individuals with crimes related to a conspiracy to steal trade secrets of an American semiconductor company for the benefit of a company controlled by the PRC government. All of the defendants were charged with a conspiracy to commit economic espionage, among other crimes. In addition, the United States filed a civil lawsuit seeking to enjoin the further transfer of the stolen trade secrets and to enjoin certain defendants from exporting to the United States any products manufactured using the trade secrets at issue. The criminal defendants are United Microelectronics Corporation (UMC), a Taiwan semiconductor foundry; Fujian Jinhua Integrated Circuit Co., Ltd. (Jinhua), a state-owned enterprise of the PRC; and three Taiwan nationals: Chen Zhengkun a/k/a Stephen Chen, age 55; He Jianting a/k/a J.T. Ho, age 42; and Wang Yungming a/k/a Kenny Wang, age 44. UMC is a publicly listed company traded on the New York Stock Exchange; is headquartered in Taiwan; and has offices worldwide, including in Sunnyvale, California. UMC mass produces integrated-circuit logic products based on designs and technology developed and provided by its customers. Jinhua is a state-owned enterprise of the PRC, funded entirely by the Chinese government, and established in February 2016 for the sole purpose of designing, developing, and manufacturing dynamic random-access memory (DRAM). According to the indictment, the defendants were engaged in a conspiracy to steal the trade secrets of Micron Technology, Inc. (Micron), a leader in the global semiconductor industry specializing in the advanced research, development, and

manufacturing of memory products, including DRAM. Micron is the only United States-based company that manufactures DRAM. Micron maintains a significant competitive advantage in this field due in large part from its intellectual property, including its trade secrets that include detailed, confidential information pertaining to the design, development, and manufacturing of advanced DRAM products. Prior to the events described in the indictment, the PRC did not possess DRAM technology, and the Central Government and State Council of the PRC publicly identified the development of DRAM and other microelectronics technology as a national economic priority. According to the indictment, Chen was a General Manager and Chairman of an electronics corporation that Micron acquired in 2013. Chen then became the president of a Micron subsidiary in Taiwan, Micron Memory Taiwan (MMT), responsible for manufacturing at least one of Micron's DRAM chips. Chen resigned from MMT in July 2015 and began working at UMC almost immediately. While at UMC, Chen arranged a cooperation agreement between UMC and Jinhua whereby, with funding from Jinhua, UMC would transfer DRAM technology to Jinhua to mass-produce. The technology would be jointly shared by both UMC and Jinhua. Chen later became the President of Jinhua and was put in charge of its DRAM production facility. While at UMC, Chen recruited numerous MMT employees, including Ho and Wang, to join him at UMC. Prior to leaving MMT, Ho and Wang both stole and brought to UMC several Micron trade secrets related to the design and manufacture of DRAM. Wang downloaded over 900 Micron confidential and proprietary files before he left MMT and stored them on USB external hard drives or in personal cloud storage, from where he could access the technology while working at UMC.

Underwater Technology to China – On Oct. 30, 2018, in the District of Massachusetts, additional charges were filed against a Chinese national in connection with violating export laws by conspiring with, among others, employees of an entity affiliated with the People's Liberation Army (PLA) in China to export illegally U.S. origin goods to China. Shuren Qin, a Chinese national residing in Wellesley, Mass., was charged in a superseding indictment with conspiracy to defraud the United States, smuggling, money laundering, and making false statements to government officials. These charges are in addition to previous charges filed, including conspiracy to commit export violations, visa fraud, and conspiracy to defraud the United States. Qin was released on conditions pending trial. According to court documents, Qin was born in the People's Republic of China and became a lawful permanent resident of the United States in 2014. Qin operates several companies in China, including a company called LinkOcean Technologies, which imports goods and technology with underwater and marine applications to China from the United States, Canada, and Europe. The indictment alleges that Qin communicated with and received taskings from entities affiliated with the PLA, including Northwestern Polytechnical University (NWPU), a Chinese military research institute, to obtain items used for anti-submarine warfare. In 2001, the Department of Commerce designated NWPU on its Entity List because of the national security risks NWPU poses to the United States. As described in the indictment, NWPU has worked closely with the PLA on the advancement of its military capabilities. Between approximately July 2015 and December 2016, it is alleged that Qin exported at least 60 hydrophones (devices used to detect and monitor sound underwater) from the United States to NWPU without obtaining the required export licenses from the Department of Commerce. Qin and his company, LinkOcean, did so by concealing from the U.S. manufacturer of the hydrophones that NWPU was the true end-user and by causing false end-user information to be filed with the U.S. Government. In addition, on four separate occasions in connection with the export of hydrophones to NWPU, Qin allegedly engaged in money laundering by transferring or causing the transfer of more than $100,000 from Chinese bank accounts to bank accounts located in the United States with the intent to promote and facilitate his unlawful export scheme. The case was investigated by Homeland Security Investigations; the Defense Criminal Investigative Service; the Department of Commerce, Office of Export Enforcement; the Federal Bureau of Investigation; and the Naval Criminal Investigative Service.

North Korea Sanctions Evasion – On Oct. 25, 2018, in the Southern District of New York, a superseding indictment was unsealed against Tan Wee Beng, a/k/a "WB," for conspiring to use the U.S. financial system

to conduct millions of dollars' worth of transactions to finance shipments of goods to the Democratic People's Republic of Korea ("DPRK" or "North Korea") by a Singapore-based commodities company ("Company-1"), of which Tan Wee Beng is a director and part-owner. Tan Wee Beng, 41, is a resident and citizen of Singapore, and remains at large. The indictment charges Tan Wee Beng with conspiring to violate United States sanctions on the DPRK by conducting those illicit transactions on behalf of North Korean entities; laundering funds in connection with those illegal transactions; defrauding several financial institutions by concealing the true nature of these transactions; and obstructing the enforcement of the sanctions regime by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). In addition to these criminal charges, OFAC designated Tan Wee Beng, Company-1, and another affiliated entity, based on the illicit support for North Korea and clandestine financial conduct charged in the indictment. According to allegations contained in the indictment: beginning in 2011, Tan Wee Beng conspired to use commodities businesses, including Company-1, of which Tan Wee Beng was both an owner and director, and front companies in Singapore, Thailand, Hong Kong, and elsewhere to violate and evade both prohibitions against North Korea's access to the U.S. financial system and prohibitions on dealings with certain North Korean entities identified by the U.S. Department of the Treasury, including Daedong Credit Bank (DCB). According to OFAC, DCB is "responsible for managing millions of dollars of transactions in support of the North Korean regime's destabilizing activities," and the United Nations reported that DCB "has knowingly facilitated transactions by using deceptive financial practices." In particular, Tan Wee Beng conspired to deceive U.S. financial institutions into conducting financial transactions on behalf of and for the benefit of DCB and other North Korean entities and persons. Those illicit transactions were used to launder money from DCB and other North Korean entities and persons to make payments to Company-1 for shipments to North Korea.

Aviation Trade Secrets to China – On Oct. 10, 2018, in the Southern District of Ohio, an indictment was unsealed charging a Chinese Ministry of State Security (MSS) operative, Yanjun Xu a/k/a Qu Hui a/k/a Zhang Hui, with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu was arrested in Belgium on April 1, 2018, pursuant to a federal complaint, and then indicted by a federal grand jury in Southern Ohio. Xu was extradited to the United States on Oct. 9, 2018. The government unsealed the charges following Xu's extradition. The four-count indictment charges Xu with conspiring and attempting to commit economic espionage and theft of trade secrets. According to the indictment: Yanjun Xu is a Deputy Division Director with the MSS's Jiangsu State Security Department, Sixth Bureau. The MSS is the intelligence and security agency for China and is responsible for counter-intelligence, foreign intelligence, and political security. MSS has broad powers in China to conduct espionage both domestically and abroad. Beginning in at least December 2013 and continuing until his arrest, Xu sought to steal trade secrets and targeted certain companies inside and outside the United States that are recognized as leaders in the aviation field. This included GE Aviation. Xu identified experts who worked for these companies and recruited them to travel to China, often initially under the guise of asking them to deliver a university presentation. Xu and others paid the experts' travel costs and provided stipends. The investigation was conducted by the FBI's Cincinnati Division, and substantial support was provided by the FBI Legal Attaché's Office in Brussels. Belgian authorities provided significant assistance in securing the arrest and facilitating the surrender of Xu. The Justice Department's Office of International Affairs provided major assistance in coordinating the extradition of Xu from Belgium.

Guns and Ammunition to Haiti – On Oct. 9, 2018, in the Northern District of Illinois, a suburban Chicago man admitted in federal court that he tried to export illegally nearly two dozen guns and ammunition to Haiti from Illinois. Patrick Germain, 45, of Evanston, Ill., pleaded guilty to one count of knowingly and fraudulently attempting to export firearms contrary to the laws and regulations of the United States. In a written plea agreement, Germain admitted that in 2016 he planned to export 16 handguns, 5 shotguns, a rifle, and ammunition from Evanston to Haiti by way of Miami, Fla. Germain built a plywood container,

filled it with the guns and ammunition, and then hid it inside a cargo van, the plea agreement states. The van was then delivered to a shipping company in Miami, but law enforcement seized it before it could be transported to Haiti. The guilty plea was entered in federal court in Chicago, and carries a maximum sentence of ten years in prison. U.S. District Judge Joan Humphrey Lefkow set sentencing for Jan. 29, 2019. According to the plea agreement, Germain in June 2016 purchased the firearms and ammunition from dealers in Illinois. Germain also purchased three vehicles, including the cargo van that he would later use to transport the concealed firearms and ammunition. He then hired an Illinois company to deliver the three vehicles to Miami, where Germain had arranged for a Florida shipping company to transport the vehicles to Haiti. When asked by the Illinois company why the cargo van appeared to be overweight, Germain represented to the driver that the added weight was due to furniture in the back seat. Germain also misled the Florida shipping company by not notifying them that the cargo van was filled with guns and ammunition, according to the plea agreement. On May 17, 2019, Judge Joan Lefkow sentenced Germain to time served. The case was investigated by the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and U.S. Immigration and Customs Enforcement's Homeland Security Investigations. Valuable assistance was provided by U.S. Customs and Border Protection and the Illinois State Police.

Electronic Devices for Cuba – On Sep. 27, 2018, in the Southern District of Florida, a Texas resident was sentenced for unlawfully exporting to Cuba electronic devices that require a license to export due to national security controls. Bryan Evan Singer, 46, of Bryan, Texas, was convicted at trial for attempting to smuggle electronics to Cuba in violation of the Cuban Embargo, and for making false statements to federal law enforcement. U.S. District Court Chief Judge K. Michael Moore sentenced Singer to 78 months in prison, to be followed by supervised release. On May 2, 2017, Singer intended to travel from Stock Island, Florida to Havana, Cuba aboard his vessel "La Mala." Prior to Singer's departure, law enforcement conducted an outbound inspection of the boat. During the inspection, Singer declared that he was only bringing to Cuba those items observable on the deck, and that the value of those items was less than $2,500. However, law enforcement conducting the search discovered a hidden compartment under a bolted down bed in the cabin of Singer's boat. In the hidden compartment, law enforcement discovered hundreds of electronic devices, valued at over $30,000. Included in those devices were over 300 Ubiquiti Nanostation Network devices, which are designed to provide highly encrypted connections between computer networks over long distances. These devices require a license for export to Cuba, under United States law, because of their national security implications. Singer never sought or obtained a license to export to Cuba, prior to his offenses of conviction. This case was investigated by the U.S. Department of Commerce, Office of Export Enforcement (OEE); U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI); and U.S. Customs and Border Protection (CBP); with assistance from the U.S. Coast Guard.

Economic Espionage by Chinese Companies – On Sep. 6, 2018, in the Northern District of California, four state-owned Chinese companies were arraigned on a Third Superseding Indictment charging each of the companies and two of their officers with conspiring to commit economic espionage and related crimes. The companies were arraigned before U.S. Magistrate Judge Donna M. Ryu on charges that the defendants conspired and attempted to engage in economic espionage by seeking to acquire misappropriated trade secrets for the production technology for chloride-route titanium dioxide (TiO2) from E.I. du Pont de Nemours & Company (DuPont). According to the original indictment that was filed January 5, 2016, between 1998 and 2011, Pangang Group Company, Ltd. – also known as Panzhihua Iron and Steel (Group) Co., Ltd. – allegedly conspired with Chinese nationals Hou Shengdong and Dong Yingjie as well as three of the company's subsidiaries and others to acquire stolen or misappropriated trade secrets. The defendant subsidiaries companies are: Pangang Group Steel Vanadium & Titanium Company, Ltd.; Pangang Group Titanium Industry Company Ltd.; and Pangang Group International Economic & Trading Company. The trade secrets relate to TiO2 technology developed by DuPont, which controlled a significant amount of the world's TiO2 sales. The defendants are alleged to have obtained confidential trade secret information

including photographs related to TiO2 plant technologies and facilities. Further, the defendants are alleged to have paid an Oakland company at least $27,000,000 between 2006 and 2011 for assistance with TiO2 technology, including obtaining DuPont trade secrets. The defendants also allegedly attempted, between 2008 and 2011, to commit economic espionage related to DuPont's TiO2 processes. In sum, the Third Superseding Indictment charges the four companies and two officers with one count of conspiracy to commit economic espionage and one count of attempted economic espionage. The indictment also seeks forfeiture of any property used in the offenses or derived from the commission of the offenses. The four companies appeared before Magistrate Judge Ryu through an attorney and pleaded not guilty to all charges. The prosecution is the result of an investigation by the Federal Bureau of Investigation.

Computer Servers to Iran – On August 17, 2018, in the Central District of California, an indictment was unsealed charging a Dana Point man with participating in a conspiracy to procure and illegally ship export-controlled computer servers to Iran. Johnny Paul Tourino, 64, was named in a 23-count grand jury indictment filed on March 7 and unsealed by a federal judge on August 17. The indictment accuses Tourino and Spectra Equipment, Inc. (Spectra), which Tourino owned and operated, with violating the International Emergency Economic Powers Act (IEEPA), which controls and restricts the export of certain goods from the United States to foreign nations. Tourino and Spectra also are charged with conspiracy, smuggling goods out of the United States, and money laundering. According to the indictment, from January 2014 through July 2017, Tourino, Spectra, and at least two others purchased and sent computer servers to Iran without obtaining licenses from the U.S. government that are required under IEEPA. The computer servers were dual-use commercial goods, meaning they had both a commercial application and a military or strategic one. The computers were controlled on the Commerce Control List for anti-terrorism and national security reasons. Tourino allegedly falsely told the manufacturer that the computer servers were intended for Kuwait and Slovenia, when he knew they were intended for Bank Mellat, an Iranian financial institution. On one occasion, according to the indictment, Tourino forwarded an email to the manufacturer after removing references to "Tehran" and "Iran." Tourino was arrested in this case on February 7, 2018, and was released on bond. Following the indictment, he was arraigned and pleaded not guilty on March 12, 2018. A trial has been scheduled for January 2020. This case is the result of an investigation conducted by the FBI, the U.S. Department of Commerce's Office of Export Enforcement, and IRS Criminal Investigation.

Defense Articles to Asia – On Aug. 6, 2018, in the District of New Mexico, Steven J. Anichowski, 26, of San Diego, Calif., was arraigned in federal court in Albuquerque, N.M., on an indictment charging him with conspiring to violate the Arms Export Control Act by scheming to export defense articles illegally to Japan, Taiwan, and Hong Kong, and other charges. The U.S. Attorney's Office announced the filing of charges against Anichowski and his co-defendants, Jonathan J. McGechie, 31, of Socorro, N.M., and Takumi Nishimori, a Japanese national. The indictment alleges that from Sep. 2010 through April 2016, Anichowski procured, sold, and shipped firearm components, defense articles and military items, which were on the U.S. Munitions List and subject to export control by the U.S. Department of State, directly and through intermediaries, to individuals in Japan, Taiwan, and Hong Kong. The indictment further alleges that Anichowski did not apply for a license or authorization from the U.S. Department of State to ship these items overseas, and did not register with the U.S. Department of State as required. According to the indictment, in January 2014, Nishimori was involved in illegally procuring firearm components from Anichowski and others in the United States and elsewhere as part of an international network that allegedly trafficked in firearm components, defense articles, and military items. The indictment alleges that Anichowski exported firearm components, defense articles, and military items to individuals, including Nishimori, using the U.S. Postal Service (USPS). It also alleges that on numerous occasions between Jan. 2014 and Aug. 2016, Anichowski directed others, including McGechie, to falsify USPS international shipment forms by falsely describing items to be shipped, undervaluing the items, and mischaracterizing the end-user information. On April 30, 2019, Anichowski pleaded guilty to illegal export and attempted

export of defense articles; he will be sentenced in December 2019. McGechie pleaded guilty to fraud and related activity in connection with computers, and was sentenced to 6 months in prison. Nishimori has yet to be arrested. The Albuquerque office of HSI and the U.S. Postal Inspection Service led the investigation of this case, with assistance from the FBI, the U.S. Department of Commerce, and the U.S. Naval Criminal Investigative Service.

Gun Parts and Ammunition to Taiwan – On July 30, 2018, in the District of Arizona, Fu Sheng Yang, 39, of Taipei City, Taiwan, was sentenced by U.S. District Judge G. Murray Snow to 33 months' imprisonment, to be followed by three years of supervised release. Yang had previously pleaded guilty to one count of attempting to smuggle goods from the United States. On June 20, 2017, Yang legally entered the United States. During the next two days, he purchased 10,000 rounds of ammunition and took possession of 40 upper receivers with the intention of illegally exporting these items from the United States to Taiwan. He also attempted to arrange for the purchase of an additional 100 firearms. On June 22, 2017, Yang was stopped by the Arizona Department of Public Safety for speeding and was found in possession of the aforementioned ammunition and upper receivers. The investigation in this case was conducted by Homeland Security Investigations, Arizona Department of Public Safety, and the Phoenix Police Department.

Sensitive Electronics to Russian Military – On July 25, 2018, in the District of New Jersey, a resident and citizen of Russia was indicted by a federal grand jury for his alleged role in an international procurement network that smuggled over $65 million worth of electronics from the United States to Russia in violation of export control laws. Alexander Brazhnikov Sr., 72, of Moscow, is charged by indictment with one count each of conspiracy to commit money laundering, conspiracy to smuggle goods from the United States, and conspiracy to violate the International Emergency Economic Powers Act (IEEPA). Brazhnikov Sr. is currently at large. According to documents filed in this case and statements made in court: Brazhnikov Sr. was the owner, chief executive officer, and principal operator of ABN Universal, a privately held Russian microelectronics import/export company in Moscow. His son, Alexander Brazhnikov Jr., 39, owned and operated four New Jersey-based microelectronics export companies in Carteret, Mountainside, Union, and Manalapan. Brazhnikov Sr. and Brazhnikov Jr. participated in a sophisticated procurement network that secretly acquired large quantities of electronic components from U.S. manufacturers and vendors and exported those parts to Russia on behalf of Russian business entities authorized to supply those parts to the Ministry of Defense of the Russian Federation, the Federal Security Service of the Russian Federation (FSB), and Russian entities involved in the design of nuclear warheads and other weapons. As part of the scheme, Brazhnikov Sr., through his Moscow business, obtained initial requests for quotes for the U.S.-based electronics components from various Russian entities and sent these requests directly to U.S.-based vendors electronically or to his son for implementation. Brazhnikov Sr., Brazhnikov Jr., and others then used Brazhnikov Jr.'s New Jersey export companies to purchase the electronic components from the U.S.-based distributors and re-package them for shipment to Moscow. In order to obscure the extent of the network's procurement activities and avoid filing the necessary export control forms, Brazhnikov Sr., Brazhnikov Jr., and others routinely falsified the true end-users and value of the components they exported. Each shipment from the United States was sent to one of 12 false addresses or shell locations in Moscow established at Brazhnikov Sr.'s direction, re-directed to a central warehouse he and others controlled, and ultimately shipped to the end-users in Russia, including the Russian defense contracting firms. Brazhnikov Jr. previously pleaded guilty to his role in the scheme and was sentenced June 30, 2016, to 70 months in prison. The case was investigated by special agents of the FBI; the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and the Department of Homeland Security, Homeland Security Investigations.

Nuclear Nonproliferation Materials to Iran – On June 20, 2018, in the Northern District of Illinois, a federal indictment was unsealed alleging an Iranian businessman's scheme to export illegally nuclear nonproliferation-controlled materials to Iran from Illinois. Saeed Valadbaigi, also known as "Saeed Valad" and "Saeed Baigi," plotted in 2011 to illegally export U.S.-origin 7075 T6 Aluminum tubing from Illinois to Iran by way of Belgium and Malaysia, the indictment states. The size and type of the aluminum was used in the missile and aerospace industry and was subject to U.S. regulations for nuclear nonproliferation purposes, the indictment states. Valadbaigi's smuggling plan was part of an effort to evade U.S. laws and export-control regulations, according to the charges. The eight-count unsealed indictment was returned in 2016 in U.S. District Court in Chicago. It charges Valadbaigi with three counts of wire fraud, two counts of attempting to violate the International Emergency Economic Powers Act, one count of conspiracy to defraud the United States, one count of illegally exporting articles from the United States, and one count of making false statements on a U.S. export form. Valadbaigi, 56, of Iran, is considered a fugitive. A warrant for his arrest was issued in 2016 and remains outstanding. In addition to the 7075 Aluminum tubing, the newly unsealed indictment accuses Valadbaigi of illegally exporting titanium sheets from a company in northern Illinois, to Iran, by way of the Republic of Georgia, the United Arab Emirates, and Malaysia. At the time of that deal in 2009, Valadbaigi controlled various companies in all three of those countries. The charges further allege that Valadbaigi in 2012 ordered acrylic sheets from a company in Connecticut, and falsely claimed that the sheets would be used only in Hong Kong. He later allegedly arranged for the acrylic sheets to be transshipped to Iran. The charges against Valadbaigi are part of an investigation that previously resulted in the conviction of Nicholas Kaiga, who managed and later owned the Belgium company that did business with Valadbaigi. Kaiga admitted in a plea agreement that he knew the 7075 Aluminum was subject to U.S. export controls and that it could not be exported to Malaysia without a license from the U.S. Department of Commerce, which neither he nor Valadbaigi possessed. Kaiga admitted that he nonetheless used his company, Industrial Metals and Commodities, as an intermediary to export the 7075 Aluminum tubing from a company in northern Illinois, to Belgium and then to Malaysia, on behalf of Valadbaigi. Kaiga pleaded guilty to violating U.S. export-control regulations and was sentenced in 2015 to two years and three months in a U.S. prison.

Jet Fuel to Syria – On June 12, 2018, in the District of Columbia, eight businessmen, including five Russian nationals and three Syrian nationals, were indicted on federal charges alleging that they conspired to violate U.S. economic sanctions against Syria and Crimea, by sending jet fuel to Syria and making U.S. dollar wire transfers to Syria and to sanctioned entities in Syria without receiving a license from the U.S. Treasury Department. The indictment was returned in U.S. District Court and involves transactions conducted by Joint Stock Company Sovfracht (Sovfracht), a Russian shipping company and freight forwarder. The five Russian nationals – Ivan Okorokov, Ilya Loginov, Karen Stepanyan, Alexey Konkov, and Liudmila Shmelkova – are employees of Sovfracht. Yaser Naser is a Syrian national who has worked on behalf of Sovfracht in Syria to coordinate its business there. Farid Bitar and Gabriel Bitar are petroleum inspectors at Port Banias, Syria. All eight individuals were charged with one count of conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and one count of conspiracy to launder monetary instruments. A forfeiture allegation was also included in the indictment. As noted in the indictment, on May 11, 2004, the President declared a national emergency to deal with the threat to the national security, foreign policy, and economy of the United States posed by the actions of the Government of Syria. That and subsequent Executive Orders imposed economic sanctions on Syria, which prohibited, among other things, the exportation, re-exportation, sale, or supply, directly or indirectly, to Syria of any goods, technology, or services from the United States, which includes the processing of U.S. dollar wires for transactions conducted overseas. According to the indictment, as early as 2011, banks began rejecting U.S. dollar wires by Sovfracht that were destined for Syria. The alleged conspirators began using front companies and falsifying information in shipping records and the related U.S. dollar wires in order to circumvent the sanctions. The indictment alleges that the defendants used vessels owned by Transpetrochart Co. Ltd. (Transpetrochart), a Russian based company that owned the petroleum tankers Mukhalatka and Yaz, to

transship jet fuel and other items surreptitiously to Syria. The indictment also notes that on May 8, 2014, the Treasury Department's Office of Foreign Assets Control (OFAC) designated the Banias Refinery Company, a Syrian based petroleum processing company owned by the Syrian regime, for processing petroleum that was imported into the Syrian Port of Banias. According to the indictment, in spite of these sanctions, the defendants engaged in U.S. dollar transactions beginning in 2015 to deliver jet fuel to Syria via the Banias Refinery Company. On or about Jan. 13, 2016, OFAC blocked two wires from Sovfracht that passed through the United States totaling $2,585,340 for the delivery of jet fuel to Syria. As a result, the defendants allegedly began to use third party companies to continue making U.S. dollar payments for shipments to Syria. On Sep. 1, 2016, OFAC designated Sovfracht for Crimean sanctions violations. Following these sanctions, Sovfracht was prohibited from transacting in U.S. dollars without first receiving a license from OFAC. On Sep. 9, 2016, the government sent notice to Sovfracht of a forfeiture action against the blocked $2,585,340. On Dec. 20, 2016, OFAC designated Transpetrochart for working with Sovfracht. According to the indictment, in October 2016, following Sovfracht's designation, the defendants utilized Maritime Assistance LLC (Maritime) as a front company for Sovfracht, as part of the scheme to circumvent U.S. sanctions and conduct U.S. dollar transactions. Maritime was operated by employees, including several of the defendants, of Sovfracht. The indictment alleges that Sovfracht and Maritime employees acted interchangeably. Maritime assumed debts previously owed by Sovfracht and paid third parties on contracts previously negotiated by Sovfracht. These activities allowed the defendants to continue engaging in U.S. dollar transactions, which passed through the United States, in spite of Sovfracht's designation. This case is being investigated by the FBI's Washington Field Office.

Night Vision Devices to Russia – On June 4, 2018, in the Southern District of Florida, Vladimir Nevidomy, 32, of Hallandale Beach, Florida, was sentenced to 26 months in prison, to be followed by three years of supervised release, for conspiring to export illegally military-grade night vision and thermal vision devices and ammunition primers to Russia. According to information contained in court documents, from as early as April 2013 through November 2013, customers in Russia contacted Nevidomy by email requesting night vision rifle scopes, thermal monoculars, and ammunition primers, all of which were on the U.S. Munitions List and subject to export control by the U.S. Department of State. Nevidomy proceeded to obtain at least three ATN MARS 4x4 night-vision riflescopes and an ODIN 61BW thermal multi-purpose monocular from U.S. vendors by falsely representing to the vendors that the items were not for export. After the U.S. vendors sent the night vision devices to Nevidomy in South Florida, he exported them to his co-defendant in Russia by either concealing the defense articles in household goods shipments sent through a freight forwarding company or using a private Russian postal service that operated in South Florida. In June 2013, Nevidomy aided and abetted the export of the ATN MARS 4x4 night-vision riflescopes from the U.S. to the co-defendant in Russia, and in August 2013, he exported the ODIN 61BW thermal multi-purpose monocular from the U.S. to the co-defendant in Russia. On or about July 19, 2013, the same co-defendant sent an email to Nevidomy requesting 1,000 large-rifle ammunition primers to be shipped to Vladivostok, Russia. On or about Oct. 2, 2013, Nevidomy attempted to export 1,000 Sellier & Bellot ammunition primers from the U.S. to the co-defendant in Vladivostok. These ammunition primers were seized by U.S. Customs and Border Protection. These night vision riflescopes, thermal monocular, and ammunition primers required a license or other authorization from the U.S. Department of State before being exported from the U.S. because they were on the U.S. Munitions List. A certified license history check revealed that neither Nevidomy, a Ukraine-born naturalized U.S. citizen, nor his associates ever applied or attempted to apply for an export license from the State Department for the night-vision equipment or ammunition primers. The case was investigated by the FBI and HSI.

Financial Transactions for Iran – On May 16, 2018, in the Southern District of New York, Mehmet Hakan Atilla was sentenced to 32 months in prison for his participation in a scheme to violate U.S. economic sanctions imposed on the Islamic Republic of Iran involving billions of dollars' worth of Iranian oil proceeds held at Atilla's employer ("Turkish Bank-1"). On Jan. 3, 2018, after a five-week jury trial, Atilla

was convicted of conspiring with others to use the U.S. financial system to conduct transactions on behalf of the government of Iran and other Iranian entities, which were barred by U.S. sanctions, and to defraud U.S. financial institutions by concealing these transactions' true nature. Atilla was sentenced by United States District Judge Richard M. Berman. According to the evidence introduced at trial, other proceedings in this case, and documents previously filed in Manhattan federal court: Beginning in or about 1979, the President, pursuant to the International Emergency Economic Powers Act (IEEPA), has repeatedly found that the actions and policies of the government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States and has declared a national emergency to deal with the threat. In accordance with these presidential declarations, the United States has instituted a host of economic sanctions against Iran and Iranian entities. This sanctions regime, among other things, prohibits financial transactions involving the United States or U.S. persons intended directly or indirectly for the government of Iran or Iranian entities. Other U.S. sanctions in effect during this case's relevant time period also required foreign financial institutions to restrict the use of Iranian oil proceeds, if those foreign banks wished to continue to do business with the U.S. financial system. Atilla and others conspired to provide access to restricted oil revenues through international financial networks, including U.S. financial institutions, to the government of Iran, Iranian entities, and entities identified by the U.S. Treasury Department's Office of Foreign Assets Control as Specially Designated Nationals (SDNs). They did so by, among other things, using Turkish Bank-1, at which Atilla served as Deputy General Manager of International Banking, to engage in transactions involving billions of dollars' worth of petroleum revenues held by the Central Bank of Iran and the National Iranian Oil Company. In particular, they facilitated and protected the ability of Turkish Bank-1 customer, international gold trader Reza Zarrab, to supply currency and gold to, and facilitate international financial transactions for, the government of Iran, Iranian entities, and SDNs using Turkish Bank-1. Many of those financial transactions involved unwitting U.S. financial institutions, in violation of U.S. sanctions against Iran. The elaborate scheme established by Atilla and others also shielded Turkish Bank-1 from U.S. sanctions. Atilla in particular lied to and deceived U.S. Treasury officials about Turkish Bank-1's activities and its purported compliance efforts in order to avoid subjecting the bank to U.S. sanctions. Additionally, Atilla, Zarrab, and others conspired to create and use false and fraudulent documents to disguise prohibited transactions for Iran and make those transactions falsely appear as transactions involving food, thus falling within humanitarian exceptions to the sanctions regime. As a result of this scheme, Atilla and his co-conspirators induced U.S. banks unknowingly to process international financial transactions in violation of IEEPA, and to launder through the U.S. financial system funds promoting the scheme.

Hundreds of Firearms to Brazil – On May 15, 2018, in the Southern District of Florida, Frederik Barbieri pleaded guilty to unlawfully exporting firearms, firearm accessories, and ammunition from South Florida to Rio de Janeiro, Brazil. Barbieri, 46, of Port St. Lucie, Florida, pleaded guilty to one count of conspiracy to commit offenses against the United States, in violation of Title 18, United States Code, Section 371, and one count of unlicensed exportation of defense articles, in violation of Title 22, United States Code, Section 2778. According to stipulated facts filed in court, from May of 2013 through February of 2018, Barbieri conspired with others to: possess firearms with obliterated serial numbers; deliver packages containing those firearms to contract carriers for international shipment without providing notice that the packages contained firearms; and smuggle firearms, firearm accessories, and ammunition from the United States to Rio de Janeiro, Brazil. During this period, a shipment sent by Barbieri was intercepted in Rio de Janeiro by Brazilian law enforcement and found to contain approximately thirty AR-15 and AK-47 rifles and firearm magazines, all concealed in four 38-gallon Rheem water heaters. The water heaters were hollowed out and loaded with the contraband, and the serial numbers on each of the firearms had been obliterated. The same day that Brazilian authorities intercepted his shipment, Barbieri called and requested that the freight forwarder destroy the related paperwork. Documentation provided by the freight forwarder revealed Barbieri's historical shipments. In addition to shipping the four Rheem water heaters in which he concealed approximately thirty rifles, Barbieri also shipped to Brazil an additional 120 Rheem water heaters, as well

as 520 electric motors and 15 air conditioning units, from May of 2013 to May of 2017, using that freight forwarder. These items are all consistent with objects used to conceal the illegal international shipment of firearms and ammunition. In February 2018, federal agents executed a warrant to search a storage unit rented by Barbieri in Vero Beach, Florida. In the storage unit, law enforcement discovered 52 rifles, 49 of which were wrapped for shipment with obliterated serial numbers. In addition, law enforcement discovered dozens of high capacity firearm magazines, over 2,000 rounds of ammunition, and packaging materials. Barbieri was arrested the following day. On July 19, 2018, U.S. District Court Judge Federico Moreno sentenced Barbieri to 154 months in prison, to be followed by supervised release. In addition, Judge Moreno entered a forfeiture money judgment against Barbieri in the amount of $9.6 million, which represents proceeds from the offenses, based on 122 shipments of water heaters containing approximately 915 firearms, and 15 shipments of air conditioning units containing approximately 45 firearms, a total of 960 firearms, with a profit of approximately $10,000 per firearm. Furthermore, the firearms and ammunition are subject to forfeiture.

Goods and Services to Iran – On April 27, 2018, in the Northern District of California, Sadr Emad-Vaez, Pouran Aazad, and Hassan Ali Moshir-Fatemi made their initial appearances in district court after being indicted on April 19, 2018, for violating export control laws under the International Emergency Economic Powers Act (IEEPA). The defendants were charged in a three-count indictment with the following crimes: conspiracy to violate the IEEPA, in violation of 50 U.S.C. §§ 1701-1705; a substantive violation of the IEEPA, 50 U.S.C. § 1705; and smuggling, in violation of 18 U.S.C. §§ 554(a) and 2. The indictment alleges the defendants engaged in transactions involving the illegal export of goods and services to Iran and financial transactions designed to evade the Iranian Transactions Sanctions Regulations (ITSR). Under the IEEPA and the ITSR, it is illegal for a United States citizen to, among other things, export, re-export, sell, or supply, directly or indirectly, any goods, technology, or services to Iran or the government of Iran, without a license granted by the Treasury Department's Office of Foreign Assets Control, or to engage in financial transactions supporting such activities. According to the indictment, the defendants, all naturalized U.S. citizens who lived variously in Tehran and the Northern District of California, participated in the operation of the Ghare Sabz Company, a/k/a GHS Technology, a large manufacturing corporation in Tehran, Iran. Emad-Vaez allegedly has described himself as the "Managing Director," Aazad as the "Chief Financial Officer," and Moshir-Fatemi as the "Engineering Manager" of the corporation. The defendants are alleged to have acquired and engaged in attempts to acquire components from manufacturers all over the world (including the U.S.), in order to funnel them to GHS in Tehran. They also allegedly used elaborate systems of international wire transfers – including through prohibited financial institutions – to fund the effort. Defendants Emad-Vaez and Aazad were arrested at their residence in Los Altos Hills on April 7, 2018, and were brought before Magistrate Judge Elizabeth D. Laporte for their initial appearance on April 9, 2018. Defendant Moshir-Fatemi was arrested near San Francisco Airport on April 11, 2018, and similarly was brought before Magistrate Laporte. All three defendants were released on secured bonds. On May 17, 2019, all three defendants pleaded guilty to conspiracy to violate the IEEPA; they will be sentenced in January 2020. The charges are the result of an investigation by agents of the Department of Commerce; Department of Homeland Security; and Internal Revenue Service, Criminal Investigation.

Aircraft Components to Iran – On April 25, 2018, in the District of New Jersey, a Morristown, N.J. woman appeared in federal court to face charges for her alleged role in an international procurement network that smuggled over $2 million worth of aircraft components from the United States to Iran in violation of export control laws. Joyce Eliabachus, a/k/a "Joyce Marie Gundran Manangan," 55, a naturalized U.S. citizen born in the Philippines, was arrested at her home on April 24, 2018, following a joint investigation by the U.S. Department of Homeland Security, Homeland Security Investigations (HSI), and the U.S. Department of Commerce, Office of Export Enforcement. Eliabachus is charged in a three-count criminal complaint with conspiracy to violate the Iranian Transactions and Sanctions Regulations (ITSR), conspiracy to commit money laundering, and conspiracy to smuggle goods from the United States. She made her initial

appearance before U.S. Magistrate Judge Mark Falk in Newark federal court and was released on $100,000 unsecured bond with home confinement. According to the complaint: Eliabachus – the principal officer and operator of Edsun Equipments LLC, a purported New Jersey-based aviation parts trading company run out of her Morristown residence – is allegedly part of a sophisticated procurement network that has secretly acquired large quantities of aircraft components from U.S. manufacturers and vendors, and exported those parts to Iran through freight-forwarding companies located in the United Arab Emirates (UAE) and Turkey, in violation of U.S. export control laws. From May 2015 through October 2017, Eliabachus and her conspirators facilitated at least 49 shipments containing a total of approximately 23,554 aircraft parts from the U.S. to Iran, all of which were exported without the required licenses. Eliabachus conspired with the owner of an Iranian-based procurement firm, identified in the complaint as "CC-1," whose international network helped initiate the purchase of U.S.-origin aircraft components on behalf of CC-1's clients in Iran. The network's client list was comprised of Iranian airline companies, several of which have been officially designated by the U.S. Government as posing a threat to the country's national security, foreign policy, or economic interests, including Mahan Air Co., Caspian Airlines, and Kish Air, among others. Using Edsun Equipments in New Jersey, Eliabachus finalized the purchase and acquisition of the requested components from the various U.S.-based distributors. She then re-packaged and shipped the components to shipping companies in the UAE and Turkey, including Parthia Cargo and Reibel Tasimacilik Ve Tic A.S., where her Iranian conspirators directed trans-shipment of the components to locations in Iran. In order to obscure the extent of the network's procurement activities, Eliabachus routinely falsified the true destination and end-user of the aircraft components she acquired. She also falsified the true value of the components being exported in order to evade the necessity of filing export control forms, which further obscured the network's illegal activities from law enforcement. The funds for the illicit transactions were obtained from the various Iranian purchasers, funneled through Turkish bank accounts held in the names of various shell companies controlled by the Iranian conspirators, and ultimately transferred into one of Edsun Equipments' U.S.-based accounts. The network's creation and use of multiple bank accounts and shell companies abroad was intended to conceal the true sources of funds in Iran, as well as the identities of the various Iranian entities who were receiving U.S. aircraft components. On June 11, 2019, Eliabachus pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act (IEEPA); she will be sentenced in February 2020.

Tactical Rifle Scope for Russia – On April 9, 2018, a Russian citizen described as a gun developer for Kalashnikov Concern – Russia's famed maker of assault rifles and a company under U.S. sanctions – pleaded guilty to a federal charge of attempting to violate U.S. export controls, according to court filings. Evgeny Viktorovich Spiridonov, 39, of Moscow, was arrested Jan. 27, 2018, at Los Angeles International Airport after leaving a major gun show in Las Vegas and attempting to board a flight for the Russian capital, according to court records. He had ordered a $2,400 restricted advanced tactical rifle scope from a Pennsylvania gun dealer, according to the filings. U.S. investigators learned of the sale from the dealer and interceded, staging a controlled delivery of the scope to Spiridonov's Las Vegas hotel, the filings said. Surveillance video showed Spiridonov accepting the shipment at the front desk. Agents then followed him as he ate breakfast, left for Los Angeles and checked his bags with the scope inside for his Aeroflot flight home, federal investigators said. Spiridonov is accused of failing to file or submitting false or misleading export information. On April 11, 2018, in the Central District of California, U.S. District Judge Manuel L. Real sentenced Spiridonov to time served. Judge Real also issued an order of removal that the defendant be removed from the United States in accordance with U.S. immigration laws and regulations.

Firearms to Romania – On April 5, 2018, in the District of Maine, Iulian Petre, a/k/a "Julian Petre," 51, of Waterville, was sentenced in U.S. District Court by Judge John A. Woodcock, Jr. to two years in prison and three years of supervised release for illegally receiving and shipping firearms. Petre was convicted of these charges on August 28, 2017, following a six-day jury trial. He was found not guilty of smuggling and money laundering charges. Court records and trial evidence revealed that in 2012 and 2013, Petre purchased

and received firearms from out-of-state sellers intending to export them unlawfully. He shipped some of these firearms to Romania. The export of these firearms required authorization from the U.S. Department of State, which the defendant knowingly failed to obtain. The investigation was conducted by U.S. Immigration and Customs Enforcement's Homeland Security Investigations; the Bureau of Alcohol, Tobacco, Firearms, and Explosives; and the U.S. Department of Commerce's Bureau of Industry and Security.

Firearm Parts to Iraq – On March 23, 2018, in the Middle District of Pennsylvania, an indictment was unsealed charging Ross Roggio, 49, of Stroudsburg, Pennsylvania, and Roggio Consulting Company LLC, a firm with which Ross Roggio was associated, for alleged involvement in a conspiracy to illegally export firearm parts, firearm manufacturing tools, and "defense services," including items used to manufacture M4 rifles, from the United States to Iraq, in violation of the Arms Export Control Act and the International Emergency Economic Powers Act. The indictment charges Ross Roggio and Roggio Consulting Company LLC with criminal conspiracy, illegal export of goods, wire fraud, and money laundering. Pursuant to regulations of the U.S. Department of Commerce, a license is required to export certain goods from the United States to Iraq for reasons of regional stability and national security. Similarly, defense services and defense articles may not be exported to Iraq without a license from the U.S. Department of State. The indictment alleges that, beginning in January of 2013 until the date of the indictment, Ross Roggio conspired to export both items and services from the United States to Iraq, without the required U.S. licenses. Conspirators allegedly purchased firearms parts and manufacturing tools from the United States and illegally exported the items to Iraq, where the items were utilized and incorporated in the manufacture and assembly of complete firearms in a plant constructed and operated in part by Ross Roggio. It is alleged that the items illegally exported included: M4 Bolt Gas Rings MIL; Firing Pin Retainers; Rifling Combo Buttons, and "defense services." The defense services allegedly provided by Ross Roggio and his firm include the furnishing of assistance to foreign persons in the manufacture of firearms. In addition to the charges relating to export controls violations, the indictment also alleges that Ross Roggio and his firm committed wire fraud on at least three occasions by purchasing items from a United States company and providing said company with false information about the end-user of the items. Finally, the indictment charges Ross Roggio and his firm with 27 counts of money laundering in the form of bank transfers from Iraq to two accounts within the Middle District of Pennsylvania, in furtherance of their unlawful export conspiracy.

Goods and Services for Syria – On March 21, 2018, in the District of Massachusetts, a Waltham, Mass. couple, their company, and a Syrian national were indicted in federal court in Boston in connection with a scheme to smuggle goods out of the United States and to supply services to Syria. Anni Beurklian, a/k/a Anni Ajaka ("Beurklian"), 49, a naturalized U.S. citizen from Lebanon who resided in Waltham; her husband, Antoine Ajaka, a/k/a Tony Ajaka ("Ajaka"), 50, a lawful permanent resident from Lebanon who resided in Waltham; Amir Katranji, a/k/a Amir Hachem Katranji, a/k/a Amir Hachem Alkatranji, a/k/a Amir Katra ("Katranji"), 52, a Syrian national; and Top Tech US Inc., a U.S. company, which operated out of the Ajaka/Beurklian residence in Waltham, were indicted on conspiracy to violate U.S. export laws and regulations, conspiracy to defraud the United States, smuggling U.S. goods out of the United States, conspiracy to obstruct justice, and obstruction of justice. Beurklian, Ajaka, and Top Tech US Inc. also are charged with illegally providing services to persons located in Syria and mail fraud. As alleged in the indictment, beginning no later than 2012 and continuing until Jan. 9, 2018, Beurklian and her husband operated an export business, Top Tech US Inc., out of their Waltham residence. The couple used their business to procure goods, including electronics, computer equipment, and electrical switches, from U.S. companies and export those goods out of the United States to customers in Lebanon and Syria. One of their customers was Amir Katranji, a citizen of Syria who operates and manages EKT Electronics (EKT), a company headquartered in Syria. In 2007, EKT and its founder, Mohammad Katranji, Amir Katranji's father, were added to the Department of Commerce's Entity List because the U.S. Government had

determined that EKT and Mohammad Katranji were involved in activities related to the acquisition, attempted acquisition, and/or development of improvised explosive devices, which were being used against U.S. and Coalition troops in Iraq and Afghanistan. As a result, since 2007, no U.S. person has been permitted to export U.S. goods to EKT without first obtaining an export license from the Department of Commerce. As alleged in the indictment, no one has sought or obtained an export license to export any U.S. goods to EKT or Mohammad Katranji. The indictment further alleges that in or about 2013, Ajaka and Beurklian began doing business with Katranji and supplying U.S. origin goods to EKT using Top Tech US. Ajaka and Beurklian knew that Katranji operated a business in Syria and that they were providing brokering services to Katranji and his Syrian company, EKT. EKT paid Ajaka and Beurklian more than $200,000 through Top Tech US bank accounts for their services. To conceal their illegal activity with EKT and evade the mandatory export filing requirement, Ajaka and Beurklian, with the knowledge and agreement of Katranji, falsified shipping paperwork and undervalued goods being shipped overseas directly to, or on behalf of, EKT. Additionally, the indictment alleges that, in or about 2016, after U.S. Government officials began detaining international shipments made by Top Tech US before they had exited the country, Beurklian, Ajaka, and Katranji conspired to obstruct justice and obstructed justice by manipulating, deleting, and falsifying records regarding shipments of U.S. goods overseas. The indictment further alleges that, on Jan. 9, 2018, after engaging in plea negotiations with the U.S. Government, Beurklian and Ajaka fled the United States to avoid prosecution. To date, they have not returned. The investigation was conducted by Homeland Security Investigations; the Federal Bureau of Investigation; the Department of Commerce, Office of Export Enforcement; and the Defense Criminal Investigative Service.

Sensitive Technology to Iran - On March 20, 2018, in the District of Minnesota, Alireza Jalali, 39, of Iran, was sentenced to 15 months in prison for his participation in a conspiracy to defraud the United States. Jalali pleaded guilty on Nov. 29, 2017. According to the defendant's guilty plea, from 2009 through December 2015, Jalali was a part-time employee of Green Wave Telecommunication, Sdn Bhn (Green Wave), a company located in Kuala Lumpur, Malaysia. Since its incorporation in 2009, Green Wave operated as a front company for Fanavar Moj Khavar (Fana Moj), an Iran-based company that specializes in both broadcast communications and microwave communications. As part of the conspiracy, Green Wave was used to acquire sensitive export-controlled technology unlawfully from the United States on behalf of Fana Moj. In order to accomplish these acquisitions, Jalali and his co-conspirators concealed the ultimate unlawful destination and end users of the exported technology through false statements, unlawful financial transactions, and other means. As part of the conspiracy, the defendant's co-conspirators would contact producers and distributors of the sought-after technology, solicit purchase agreements, and negotiate the purchase and delivery of the goods with the seller. When the goods were received by Green Wave in Malaysia, Jalali repackaged and unlawfully exported the items from Malaysia to Fana Moj in Tehran, Iran. In 2017, Fana Moj was designated by the U.S. Department of the Treasury as a Specially Designated National for providing financial, material, technological or other support for, or goods or services in support of, the IRGC. On Sep. 24, 2019, Iranian citizen Negar Ghodskani, 40, was sentenced to 27 months in prison for her participation in this conspiracy. Ghodskani, who pleaded guilty on Aug. 9, 2019, was sentenced before United States District Judge Joan N. Ericksen in Minneapolis. This case is the result of an investigation conducted by the FBI, the U.S. Department of Commerce-OEE and HSI.

Millions of U.S. Dollars to Iran – On March 20, 2018, the U.S. Attorney's Office for the Southern District of New York announced the arrest of Ali Sadr Hashemi Nejad ("Sadr") for his alleged involvement in a scheme to evade U.S. economic sanctions against Iran, to defraud the United States, and to commit money laundering and bank fraud. Sadr was charged with participating in a scheme in which more than $115 million in payments for a Venezuelan housing complex were funneled illegally through the U.S. financial system for the benefit of Iranian individuals and entities. Sadr was arrested on March 19 on a six-count Indictment and presented in U.S. District Court for the Eastern District of Virginia. Sadr, 38, of Iran, is charged with one count of conspiracy to defraud the United States, one count of conspiracy to violate the

International Emergency Economic Powers Act (IEEPA), one count of bank fraud, one count of conspiracy to commit bank fraud, one count of money laundering, and one count of conspiracy to commit money laundering. Sadr's case has been assigned to U.S. District Judge Andrew L. Carter Jr. in the Southern District of New York. According to the Indictment unsealed in Manhattan federal court: Beginning in 1979, the President of the United States, pursuant to the IEEPA, has repeatedly found that the actions and policies of the government of Iran constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States and declared a national emergency to deal with the threat. In accordance with these presidential declarations, the United States has instituted a host of economic sanctions against Iran and Iranian entities. In August 2004, the governments of Iran and Venezuela entered into an agreement (the "Agreement"), whereby they agreed to cooperate in certain areas of common interest. The following year, both governments supplemented the Agreement by entering into a Memorandum of Understanding regarding an infrastructure project in Venezuela (the "Project"), which was to involve the construction of thousands of housing units in Venezuela. The Project was led by Stratus Group, an Iranian conglomerate controlled by Sadr and his family with international business operations in the construction, banking, and oil industries. In December 2006, Stratus Group incorporated a company in Tehran, which was then known as the Iranian International Housing Corporation (IIHC). IIHC was responsible for construction for the Project. Thereafter, IIHC entered into a contract with a subsidiary of a Venezuelan state-owned energy company (the "VE Company"), which called for IIHC to build approximately 7,000 housing units in Venezuela in exchange for approximately $475,734,000. Stratus Group created the Venezuela Project Executive Committee to oversee the execution of the Project. Sadr was a member of the committee and was responsible for managing the Project's finances. In connection with his role on the Project, Sadr took steps to evade U.S. economic sanctions and to defraud U.S. banks by concealing the role of Iran and Iranian parties in U.S. dollar payments sent through the U.S. banking system. For example, in 2010, Sadr and a co-conspirator used St. Kitts and Nevis passports and a United Arab Emirates address to incorporate two entities outside Iran that would receive U.S. dollar payments related to the Project on behalf of IIHC. The first entity, Clarity Trade and Finance ("Clarity"), was incorporated in Switzerland, and the second, Stratus International Contracting, J.S., a/k/a "Stratus Turkey," a/k/a "Straturk," was incorporated in Turkey. Stratus Turkey and Clarity were both owned and controlled by Sadr and his family members in Iran. Sadr then opened U.S. dollar bank accounts for Clarity and Stratus Turkey at a financial institution located in Switzerland. Thereafter, Sadr and others conducted a series of international financial transactions using Clarity and Stratus Turkey for the benefit of Iranian parties in a manner that concealed the Iranian nexus to the payments, in violation of U.S. economic sanctions. Specifically, between April 2011 and November 2013, the VE Company, at the direction of Sadr and others, made approximately 15 payments to IIHC through Stratus Turkey or Clarity, totaling approximately $115,000,000. Sadr and others directed that payments be routed through banks in the United States to Stratus Turkey's or Clarity's bank accounts at the financial institution in Switzerland. The majority of the funds were then transferred to another offshore entity located in the British Virgin Islands, which had been incorporated by Sadr and others in 2009. In addition, on February 1, 2012, Clarity wired more than $2,000,000 of proceeds from the Project directly into the United States. Those proceeds were then used to purchase real property in California.

Petrochemical Parts for Iran - On March 14, 2018, in the Western District of Washington, a Canadian citizen was arrested on arrival at Sea-Tac Airport following his indictment on charges of violating U.S. export laws and making false statements to federal investigators. Mehran Ghanouni, 29, operated a number of companies in both the U.S. and Canada. The indictment alleges that between 2014 and 2016, Ghanouni and his co-conspirators exported $2.3 million in parts for petrochemical operations, falsely claiming they were destined for companies in Kuwait, Iraq, and the United Arab Emirates (UAE). In fact, the co-conspirators knew the equipment was to be transshipped to oil companies owned by the government of Iran. Such exports are illegal under federal law. According to the indictment, the co-conspirators attempted to export the equipment illegally on 35 different occasions. The indictment describes a February 2014 export where Ghanouni's company, Integrated Control Systems (ICS), claimed the parts were for an oil

refinery in Kuwait when in fact they were destined for Iran. In May 2014, ICS claimed parts were destined for a company in Iraq, when in fact they were for an Iranian oil company. In December 2014, U.S. Customs and Border Protection seized a shipment of parts ICS was sending overseas, suspecting they were headed to Iran; the company claimed they were for repairs to be made in the UAE for a project in Iraq. Other shipments in January 2015 and February 2016 also allegedly were destined for Iran, but were represented as being for companies in Iraq and the UAE. When questioned, Mehran Ghanouni told a special agent with Homeland Security Investigations that his company did not do any business with Iran. On August 10, 2018, Mehran Ghanouni was acquitted of the charges alleged in the indictment. Arrest warrants have been issued for two co-conspirators, Bahram Ghanouni a/k/a Ben Anderson and Peiman Basiri. The case was investigated by U.S. Immigration and Customs Enforcement's Homeland Security Investigations and the U.S. Department of Commerce, Office of Export Enforcement.

Unlawful Exports to Pakistan – On March 5, 2018, in the District of Connecticut, Muhammad Ismail, 67, and Kamran Khan, 38, pleaded guilty in Bridgeport federal court to money laundering in connection with funds they received for the unlawful export of goods to Pakistan. A third defendant, Imran Khan, 43, previously pleaded guilty to violating U.S. export laws. According to court documents and statements made in court, from at least 2012 to December 2016, Ismail, and his two sons, Kamran and Imran Khan, were engaged in a scheme to purchase goods that were controlled under the Export Administration Regulations (EAR) and to export those goods without a license to Pakistan, in violation of the EAR. Through companies conducting business as Brush Locker Tools, Kauser Enterprises-USA, and Kauser Enterprises-Pakistan, the three defendants received orders from a Pakistani company that procured materials and equipment for the Pakistani military, requesting them to procure specific products that were subject to the EAR. When U.S. manufacturers asked about the end-user for a product, the defendants either informed the manufacturer that the product would remain in the U.S. or completed an end-user certification indicating that the product would not be exported. After the products were purchased, they were shipped by the manufacturer to the defendants in Connecticut. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission (PAEC), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics (NILOP), all of which were listed on the U.S. Department of Commerce's Entity List. The defendants never obtained a license to export any item to the designated entities even though they knew that a license was required prior to export. On July 18, 2018, U.S. District Judge Stefan R. Underhill sentenced both Muhammad Ismail and Kamran Khan to 18 months imprisonment followed by three years of supervised release.

Equipment, Firearms, and Ammo to Ukraine – On February 28, 2018, in the Western District of Pennsylvania, one Michigan resident and one New Jersey resident were indicted by a federal grand jury on a charge of conspiracy. The one-count indictment named Michael Cox, 42, of Beverly Hills, Michigan, and Michael Stashchyshyn, 55, of Cedar Knolls, New Jersey, as defendants. According to the indictment, Cox and Stashchyshyn conspired with others to export night sighting equipment, firearms, and ammunition to Ukraine without the requisite license. The items were purchased in the United States by Cox and others, and shipped to Stashchyshyn who owns a freight forwarder business in Parsippany, New Jersey. Stashchyshyn then shipped the items to an individual in Ukraine in violation of U.S. law and regulations. The items shipped are on the U.S. Munitions List and are controlled by the International Traffic in Arms Regulations (ITAR). Such items are illegal to ship without a license from the Department of State, which the defendants and their co-conspirators did not have. U.S. Immigration and Customs Enforcement / Homeland Security Investigations and the United States Postal Inspection Service conducted the investigation leading to the indictment in this case.

Firearms for Chechnya – On Feb. 27, 2018, in the Eastern District of Virginia, two Alexandria residents were arrested on charges of international trafficking in firearms, smuggling, and other charges. According to allegations in the criminal complaint, Tengiz Sydykov, 28, and Eldar Rezvanov, 27, each citizens of

Kyrgyzstan residing in Alexandria, purchased over 100 disassembled firearms and attempted to ship them to Chechnya without a license. The men attempted to smuggle the firearms to Chechnya by using false shipping inventories and disguising the disassembled firearms as kitchen utensils. Sydykov and Rezvanov were charged with Violating the Arms Export Control Act, Conspiracy to Smuggle Goods from the United States, Wire Fraud, Bank Fraud, and Money Laundering. On May 10, 2018, Rezvanov pleaded guilty to a violation of the Arms Export Control Act; he was sentenced to 46 months in prison. On Sep. 21, 2018, Sydykov pleaded guilty to violating the Arms Export Control Act; he was sentenced to 36 months in prison. Both defendants face deportation upon completion of their prison terms. The investigation was conducted by U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI).

Goods and Technology to Hizballah - On Feb. 16, 2018, the District of Minnesota announced the indictment of Usama Darwich Hamade, 53, Samir Ahmed Berro, 64, and Issam Darwich Hamade, 55, for conspiring to export goods and technology illegally from the United States to Lebanon and to Hizballah. Defendants Usama Hamade and Issam Hamade were arrested in South Africa, and in October 2019 they were extradited to the United States. Samir Ahmed Berro remains at large. According to the Indictment, from 2009 through December 2013, Usama Hamade, Berro, and Issam Hamade willfully conspired to export and attempted to export from the United States to Lebanon, and specifically to Hizballah, goods and technology without obtaining the required export licenses from the U.S. Department of Commerce and the U.S. Department of State, in violation of the International Emergency Economic Powers Act, the Export Administration Regulations, the Arms Export Control Act, and the International Traffic in Arms Regulations. According to the Indictment, the defendants caused the export of inertial measurement units (IMUs) suitable for use in unmanned aerial vehicles (UAVs), a jet engine, piston engines, and recording binoculars to Hizballah, designated by the U.S. Secretary of State as a "foreign terrorist organization." As part of the conspiracy, in October 2009, Usama Hamade directed Individual A to order the jet engine and have it delivered to SAB Aerospace, a company owned by Berro in the United Arab Emirates. Berro then transshipped the jet engine to Hizballah co-conspirators in Lebanon. In September 2009 through November 2009, Usama Hamade directed Individual A to place orders for digital compasses and the IMUs for delivery to South Africa, falsely telling Individual A that the parts would be used in UAVs in South Africa to fly over wildlife areas to prevent poaching. Instead, Usama Hamade transshipped the digital compasses and the IMUs to Hizballah co-conspirators in Lebanon. This case is the result of an investigation conducted by the FBI, the Department of Commerce's Office of Export Enforcement, and Homeland Security Investigations.

Arms and Munitions to Thailand – On Jan. 23, 2018, in the District of Maryland, a federal grand jury indictment was unsealed charging Thai national Apichart Srivaranon, age 32, of Patumthanee Province, Thailand, for a conspiracy, between 2012 and 2016, to export unlawfully arms and munitions from the United States to Thailand and witness tampering. The indictment was returned on Nov. 9, 2016, and was unsealed upon the arrest of Srivaranon in Las Vegas, Nevada. The case against Srivaranon was assigned to U.S. District Court Judge George J. Hazel of the District of Maryland. According to the five-count indictment, Srivaranon obtained firearm parts in the United States that are listed on the United States Munitions List and exported them to Thailand without having first obtained the required license or written authorization from the Directorate of Defense Trade Controls, an office in the U.S. Department of State. In furtherance of the conspiracy, Srivaranon purchased firearms parts online from United States gun manufacturers. These firearms parts included key components for AR-15 and M-16 military-style assault rifles. Srivaranon then had the firearms parts sent to addresses in the United States where his co-conspirators lived, visited, or conducted business, including Ohio, New York, Maryland, and Nevada. Srivaranon recruited his co-conspirators, often Thai women who were living in the United States for the first time as au pairs and, in one instance, a University of Maryland college student, through social media. Upon receipt of the munitions, Srivaranon directed his co-conspirators to repackage the parts and falsely label United States Postal Service (USPS) customs forms. Srivaranon also directed his co-conspirators to falsely declare

the contents of these packages upon shipment, listing the contents as spare parts, bicycle parts, fishing parts, or toy parts, and then ship them to Thailand via the USPS and private shipping companies. To avoid detection, Srivaranon instructed his co-conspirators to alternate the frequency and addresses of shipments, as well as the estimated value of the contents of the shipments. Srivaranon is charged with: (1) conspiracy to violate the Arms Export Control Act (AECA); (2) three substantive AECA violations for attempts to export firearms parts to Thailand in September 2013 and October 2013; and (3) tampering with a witness. On Jan. 8, 2019, Srivaranon pleaded guilty to conspiracy to unlawfully export arms and munitions, and unlawfully exporting arms and munitions. On April 16, 2019, he was sentenced to 26 months in prison and forfeiture of $10,000 in U.S. currency. This case is the result of an investigation conducted by ICE-HSI, ATF, and U.S. Customs and Border Protection, with valuable assistance provided by Thailand's Department of Special Investigation.

Microwave Integrated Circuits for China - On Jan. 19, 2018, in the Central District of California, Yi-Chi Shih, an electrical engineer who is a part-time Los Angeles resident, and Kiet Ahn Mai a/k/a Kiet Anh Mai were arrested pursuant to a criminal complaint. The complaint alleges that Shih and Mai conspired to provide Shih with unauthorized access to a protected computer of a United States company that manufactured specialized, high-speed computer chips known as monolithic microwave integrated circuits (MMICs). The conspiracy count also alleges that the two men engaged in mail fraud, wire fraud, and international money laundering to further the scheme. It also alleges that Shih violated the International Emergency Economic Powers Act (IEEPA). The complaint affidavit alleges that Shih and Mai executed a scheme to defraud the U.S. company out of its proprietary, export-controlled items, including technology associated with its design services for MMICs. The victim company's proprietary semiconductor technology has a number of commercial and military applications, and its customers include the Air Force, Navy, and the Defense Advanced Research Projects Agency. MMICs are used in electronic warfare, electronic warfare countermeasures, and radar applications. As part of the scheme, Shih and Mai accessed the victim company's computer systems via its web portal after Mai obtained that access by posing as a domestic customer seeking to obtain custom-designed MMICs that would be used solely in the United States. Shih and Mai allegedly concealed Shih's true intent to transfer the U.S. company's technology and products to the People's Republic of China, and specifically to Chengdu GaStone Technology Company (CGTC), a Chinese company which was placed on the Commerce Department's Entity List in 2014. Shih is a former president of CGTC. On Dec. 6, 2018, Mai pleaded guilty to smuggling goods to China. Mai was sentenced to 18 months' probation and fined $5,000. On June 26, 2019, a jury found Shih guilty of conspiracy to violate the IEEPA, mail fraud, wire fraud, subscribing to a false tax return, making false statements to a government agency, and conspiracy to gain unauthorized access to a protected computer to obtain information. Shih's sentencing date is to be determined.

Night Vision Military Technology to Italy – On Dec. 21, 2017, in the Eastern District of New York, Giovanni Zannoni, an Italian national and member of the Italian armed services, pleaded guilty to illegally exporting controlled military technology from the United States to Italy. As part of his plea, Zannoni agreed to forfeit $436,673, in addition to the dozens of gun parts and night vision and thermal imaging devices recovered by the government in connection with this prosecution. According to court filings and admissions made in court at the time he entered the guilty plea, between June 2013 and May 2017 Zannoni illegally exported and attempted to export night vision goggles and assault rifle components designated as defense articles on the United States Munitions List. The export of sensitive night vision equipment and assault rifle components requires a license from the U.S. Department of State. On May 14, 2017, the defendant was arrested after entering the United States at Miami International Airport. On Feb. 22, 2018, Zannoni was sentenced to 11 months in prison. This case was investigated by the Department of Defense, Defense Criminal Investigative Service, Northeast Field Office (DCIS); U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI); and the U.S. Attorney's Office.

U.S. Military Technology to IRGC - On Dec. 15, 2017, in the Southern District of New York, Ali Soofi, a Canadian-Iranian dual citizen, was sentenced to 32 months in prison for his participation in a conspiracy to violate the International Emergency Economic Powers Act (IEEPA). Soofi was charged and arrested by special agents of the Federal Bureau of Investigation (FBI) following an investigation. Soofi pleaded guilty to one count of conspiracy to violate IEEPA on September 7, 2017, before U.S. District Judge Nelson S. Román, who imposed the sentence. Between 2014 and December 2016, Soofi conspired to export military items from the United States to Iran, both directly and through transshipment to intermediary countries, without a license. In particular, Soofi acted as a broker on behalf of Iranian clients, including a high-ranking official in the Iranian Revolutionary Guard Corps (IRGC), who sought American military technology. Over the course of the conspiracy, Soofi sought to purchase and ship numerous items, including helicopters, high-tech machine gun parts, tank parts, and military vehicles, from the United States to Iran, all without a license and while knowing that such shipments were illegal under U.S. law. During the multi-year conspiracy, Soofi worked to fill specific orders for the IRGC by contacting other individuals with access to the requested military items through email, phone, and in-person meetings. The IRGC has been designated as a Specially Designated Global Terrorist for its activities in support of terrorist groups including Hezbollah, Hamas, and the Taliban. One of Soofi's customers was a Commander in the IRGC, who acted as a key figure at the Iranian Ministry of Defense responsible for procurement of parts and weapons. Among the weapons Soofi sought on behalf of the IRGC were dampeners – or shock absorbers – which allow high-tech machine guns to be mounted on helicopters and boats. In addition, Soofi sought to obtain slewing rings for tanks, military helicopters, target sights, jet engines, and military vehicles such as Humvees for the IRGC. In addition to the prison term, Soofi, 63, was sentenced to one year of supervised release.

Marine Products for Iranian Navy - On Dec. 11, 2017, in the Eastern District of Wisconsin, Resit Tavan, age 40, of Istanbul, Turkey, was arraigned in federal court in Milwaukee on an indictment returned June 27, 2017. Tavan, owner and president of Ramor Dis Ticaret, Ltd. (Ramor), a Turkish company, and Fulya Oguzturk are charged, along with Ramor, with conspiring to defraud the United States and to smuggle American made products to Iran in violation of the International Emergency Economic Powers Act (IEEPA). The indictment charges that Tavan, Oguzturk, and Ramor arranged the purchase and acquisition of marine products manufactured in Wisconsin, for shipment to and use by Iran. The indictment alleges that the goods, specifically outboard engines, generators, and propulsion systems, were shipped first to Turkey and then to Iran without the knowledge of the manufacturers, and without the permission and license of the United States. The indictment further alleges that the marine products were intended for use by the Iranian navy. In addition to the conspiracy charge, the indictment charges three counts of violating IEEPA; three counts of smuggling; and six counts of money laundering. Tavan was arrested in Romania in June 2017, on an international arrest warrant issued at the request of the United States. Upon his arrest, the United States requested Tavan's extradition from Romania. He was extradited from Romania to the United States in December 2017. On April 2, 2019, Tavan pleaded guilty to a conspiracy to violate U.S. sanctions on Iran under the IEEPA. On Aug. 29, 2019, Tavan was sentenced to 27 months in prison. This case was investigated by the Federal Bureau of Investigation and the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement.

Aviation Parts and Equipment to Syria - On Oct. 3, 2017, in the Southern District of Florida, three Miami-Dade County residents, Ali Caby, a/k/a "Alex Caby," 40, Arash Caby, a/k/a "Axel Caby," 43, and Marjan Caby, 34, pleaded guilty to Count 1 of an Indictment charging them with conspiracy to defraud the United States and to illegally export aviation parts and equipment to Syria in violation of the International Emergency Economic Powers Act (IEEPA). The exports were sent to Syrian Arab Airlines, a/k/a "Syrian Air," which had been designated as a Specially Designated National (SDN) by the U.S. Department of Treasury, Office of Foreign Assets Control (OFAC). U.S. persons and entities are prohibited from doing business with SDNs, such as Syrian Air, without obtaining a license from OFAC. According to court

documents, Ali Caby ran the Bulgaria office of AW-Tronics, a Miami export company that was managed by Arash Caby, and which shipped and exported various aircraft parts and equipment to Syrian Air. Ali Caby and Arash Caby closely supervised and encouraged subordinate employees of AW-Tronics in the willful exportation of the parts and equipment to SDN Syrian Air. Marjan Caby, as AW-Tronics' export compliance officer and auditor, facilitated these exports by submitting false and misleading electronic export information to federal agencies. On Dec. 19, 2017, Ali Caby was sentenced to 24 months in prison and forfeiture of $17,500; Arash Caby was sentenced to 24 months in prison and fined $10,000; and Marjan Caby was sentenced to 1 year and 1 day in prison.

U.S. Army Equipment on eBay – On Sep. 1, 2017, in the Middle District of Tennessee, John Roberts, 27, of Clarksville, Tenn., was found guilty by a federal jury of conspiracy to steal and sell U.S. Army property, 10 counts of wire fraud, and two counts of violating the Arms Export Control Act. The jury returned a verdict of guilty on all counts, after a four-day trial in U.S. District Court. Roberts is the final defendant convicted in the conspiracy, after an indictment issued in October 2016 charged six U.S. Army soldiers and two civilian eBay sellers with various crimes. The Court remanded Roberts to the custody of the U.S. Marshal following the verdict. According to the proof at trial, Roberts conspired with the soldiers, who stole U.S. Army equipment, often after hours, from the U.S. Army installation at Fort Campbell. Roberts then purchased the equipment from the soldiers, often times in dark parking lots and by cash only transactions. Roberts knew that some of the soldiers had financial problems or serious drug addictions. Roberts then resold this military grade equipment via eBay. The U.S. Army equipment listed for sale on eBay included sniper telescopes and other sniper rifle accessories, parts for the M249 machine gun (including barrel assemblies, trigger groups, rail adapter kits, magazine buttstocks, mounts, and heat shields), sights for the M203 grenade launcher, "red dot" sights for the M2 rifle and M4 assault rifle, flight helmets, communications headsets, and medical supplies. Further proof at trial established that Roberts illegally exported certain restricted U.S. Army equipment, including night vision helmet mounts, and that Roberts sold U.S. Army equipment to eBay customers around the world, including customers in Russia, China, Thailand, Japan, the Netherlands, Australia, India, Germany, and Mexico. Six co-defendant's previously pleaded guilty. On Dec. 21, 2016, former U.S. Army Specialist Dustin Nelson, 23 of Northville, New York pleaded guilty to conspiracy to steal and sell U.S. Army property. On Feb. 8, 2016, former U.S. Army Specialist Kyle Heade, 30, formerly of Fort Campbell, Kentucky, pleaded guilty to conspiracy to steal and sell U.S. Army property. On March 30, 2016, former U.S. Army Sergeant Michael Barlow, 30, of Clarksville, Tenn., pleaded guilty to conspiracy to steal and sell U.S. Army property and theft of government property. On April 6, 2017, Cory Wilson, 43, of Gonzalez, Louisiana, pleaded guilty to conspiracy to steal and sell U.S. Army property, wire fraud, and violating the Arms Export Control Act. On April 26, 2017, Jonathan Wolford, 29, of Clarksville, Tenn., pleaded guilty to conspiracy to steal and sell U.S. Army property. On April 26, 2017, Alexander Hollibaugh, formerly of Fort Campbell, Kentucky, pleaded guilty to conspiracy to steal and sell U.S. Army property. On Dec. 5, 2017, Roberts was sentenced to 180 months in prison and $4,270,000 restitution.

Firearms to Dominican Republic - On Aug. 25, 2017, in the Southern District of Florida, former Miami-Dade Police Department (MDPD) officer Michael Freshko, 48, was sentenced to four years in prison after previously pleading guilty to conspiracy to unlawfully export firearms from the United States to the Dominican Republic, on flights from Miami International Airport. According to the court record, after receiving firearms from a co-conspirator, Freshko used his official position as a MDPD officer to transport the firearms past the passenger screening area and into the portion of Miami International Airport that housed the departure gates. Freshko thereafter would deliver the firearms to a co-conspirator, who in turn would store the firearms within carry-on baggage. Next, a co-conspirator would travel to the Dominican Republic aboard a commercial flight, with the firearms in carry-on baggage. After arriving in the Dominican Republic, a co-conspirator would deliver the firearms to an associate. Freshko further admitted that one or more firearms were smuggled in this manner in October 2012, and multiple firearms were smuggled in

December 2012. The smuggled firearms included four Glock .9 mm pistols, one Sig Sauer .9 mm pistol, and one Sig Sauer 5.56 rifle.

Integrated Circuits to Russia and China - On Aug. 3, 2017, in the Eastern District of Texas, Peter Zuccarelli pleaded guilty to conspiring to smuggle and illegally export radiation hardened integrated circuits (RHICs) from the United States, for use in the space programs of China and Russia, in violation of the International Emergency Economic Powers Act (IEEPA). Zuccarelli pleaded guilty to engaging in a conspiracy to smuggle and illegally export U.S. items subject to IEEPA, without obtaining licenses from the Department of Commerce. According to the allegations contained in the Information filed against Zuccarelli and statements made in court filings and proceedings: Between approximately June 2015 and March 2016, Zuccarelli and his co-conspirator agreed to illegally export RHICs to China and Russia. RHICs have military and space applications, and their export is strictly controlled. In furtherance of the conspiracy, Zuccarelli's co-conspirator received purchase orders from customers seeking to purchase RHICs for use in China's and Russia's space programs. Zuccarelli received these orders from his co-conspirator, as well as payment of approximately $1.5 million to purchase the RHICs for the Chinese and Russian customers. Zuccarelli placed orders with U.S. suppliers, and used the money received from his co-conspirator to pay the U.S. suppliers. In communications with the U.S. suppliers, Zuccarelli certified that his company, American Coating Technologies, was the end user of the RHICs, knowing that this was false. Zuccarelli received the RHICs he ordered from U.S. suppliers, removed them from their original packaging, repackaged them, falsely declared them as "touch screen parts," and shipped them out of the United States without the required licenses. In an attempt to hide the conspiracy from the U.S. Government, he created false paperwork and made false statements. On Jan. 24, 2018, Zuccarelli was sentenced to 46 months in prison, three years' supervised release, and a $50,000 fine. This case was investigated by the Dallas and Denver Offices of the Department of Homeland Security, Homeland Security Investigations; the Federal Bureau of Investigation; Internal Revenue Service - Criminal Investigation; Postal Inspection Service; the Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and the Defense Criminal Investigative Service.

Rifle Scopes and Tactical Equipment to Syria - On Aug. 1, 2017, in the Central District of California, the chief executive officer of an Orange County check-cashing business was arrested on charges of procuring and illegally exporting rifle scopes, laser boresighters, and other tactical equipment from the United States to Syria in violation of the International Emergency Economic Powers Act (IEEPA). Rasheed Al Jijakli, 56, a Syrian-born naturalized U.S. citizen, was arraigned on a three-count indictment that was returned by a federal grand jury on July 14. The indictment was unsealed after Jijakli was taken into custody without incident by law enforcement authorities. The indictment accuses Jijakli of violating IEEPA, which authorizes the president to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy or economy of the United States. In accordance with that authority, the president issued an executive order that included broad restrictions on exports to Syria. The Department of Commerce subsequently issued corresponding regulations restricting exports to Syria of items subject to the Export Administration Regulations. Jijakli also faces charges of conspiring to violate IEEPA and smuggling. From January 2012 through March 2013, Jijakli and three other individuals purchased and smuggled export-controlled items to Syria without obtaining licenses from the Department of Commerce. Jijakli and others allegedly hand-carried the items through Istanbul, Turkey and provided them to fighters in Syria. Those items allegedly included day- and night-vision rifle scopes, laser boresighters (tools used to adjust sights on firearms for accuracy when firing), flashlights, radios, a bulletproof vest and other tactical equipment. On August 13, 2018, Jijakli pleaded guilty to a felony conspiracy charge and admitted he conspired with others to export tactical gear from the United States to Syria. On December 20, 2018, Jijakli was sentenced by United States District Judge James V. Selna to 46 months in federal prison. This case is the result of an investigation by the FBI, U.S. Immigration and

Customs Enforcement's Homeland Security Investigations, the U.S. Department of Commerce's Office of Export Enforcement, and IRS Criminal Investigation.

Accelerometers and Gyroscopes for China - On July 27, 2017, in the Western District of Washington, a resident of New Zealand, who traveled to Seattle in April 2016 to take possession of export-restricted parts designed for missile and space applications, was sentenced in U.S. District Court to two years in prison for conspiring to violate the Arms Export Control Act. William Ali, 38, had been in federal custody since his arrest on April 11, 2016. According to records in the case and testimony presented at trial, Ali emailed several companies and distributors in April 2015 about purchasing certain accelerometers that are designed for use in spacecraft and missile navigation. These accelerometers cannot be exported from the United States without a license from the U.S. State Department, which Ali did not have. Homeland Security Investigations (HSI) learned of Ali's inquiries and began an investigation. Over the next year, Ali communicated by phone and email with an HSI undercover agent, and with a person in China known in his emails as "Michael." Michael was the person seeking the accelerometers, as well as certain gyroscopes that are designed for military use. Ali was working to find a way to purchase the devices and transport them secretly to Michael in China. In multiple emails, Ali made clear that he was aware that export of the accelerometers and gyroscopes was illegal. Ali sent the undercover agent nearly $25,000 for the devices – money he got from Michael. Ali traveled to Seattle and met with the undercover agent on April 11, 2016, at a downtown hotel. Shortly after Ali took possession of the devices, he was arrested. Ali had with him an airline ticket to Hong Kong and a visa to travel to China. This case was investigated by U.S. Immigration and Customs Enforcement's Homeland Security Investigations.

Memory Chip Modules to Russia - On July 19, 2017, in the District of Colorado, an indictment was unsealed charging Bulgarian citizen Tsvetan Kanev with smuggling and violations of the International Emergency Economic Powers Act (IEEPA). Kanev is a fugitive. According to the indictment, from mid-2015 and continuing through June 2016, Kanev unlawfully and willfully attempted to export and cause to be exported from the United States to Russia items on the Commerce Control List (CCL) without having first obtained the required authorization and license from the U.S. Department of Commerce. CCL items include those that could make a significant contribution to the military potential or nuclear proliferation of other nations or that could be detrimental to the foreign policy or national security of the United States. Specifically, Kanev exported static random access memory multi-chip modules, clock drivers (used to optimize timing of high performance microprocessors and communications systems), and multiple analog-to-digital converters.

Sophisticated Machinery to Iran - On July 17, 2017, in the District of Columbia, Joao Pereira da Fonseca, 55, a citizen of Portugal, pleaded guilty to a federal charge stemming from a scheme in which he conspired to help an Iranian company unlawfully obtain sophisticated equipment from two companies in the United States. Fonseca, of Coimbra, Portugal, pleaded guilty to conspiring to unlawfully export goods and technology to Iran and to defraud the United States. On Sep. 14, 2017, Fonseca was sentenced to 20 months in prison. Upon completion of his prison term, Fonseca faces deportation proceedings. At the time he entered his guilty plea, Fonseca admitted to taking part in the scheme between October 2014 and April 2016. One of the companies in the United States manufactures machines that help produce sophisticated optical lenses that have both commercial and military uses. The other company manufactures machinery that tests components of inertial guidance systems that have both commercial and military uses. Fonseca was a contractor for a Portuguese engineering company that served as a front company to purchase the machines on behalf of their Iranian client. The Portuguese company claimed that it was purchasing the machines for its own use, but it in fact planned to have the machines shipped to Iran. Fonseca is a mechanical engineer whose role in the conspiracy was to travel to the U.S. to approve the machinery and learn how to install and maintain the machinery once it was shipped to its final destination in Iran. Due to the investigation conducted by a special agent from Homeland Security Investigations, the government

prevented both machines from leaving the U.S. Fonseca traveled to the United States to receive training on how to use the optical lens equipment in October 2015. He returned to the United States in late March 2016 to be trained on how to use the inertial guidance system equipment at the company that manufactures it. After a week of training, Homeland Security agents had gathered sufficient evidence to detain Fonseca before he could fly back to Portugal. Soon thereafter, criminal charges were brought against Fonseca. He has been in custody ever since.

Industrial Goods to Iran - On June 21, 2017, in the Northern District of Ohio, an indictment was unsealed charging IC Link Industries Ltd., Mohammad Khazrai Shaneivar, Arezoo Hashemnejad Alamdari, and Parisa Mohamadi a/k/a Parisa Javidi with conspiracy to export goods from the United States to Iran without the required license by the Department of the Treasury, Office of Foreign Assets Control, and to prevent officials of the U.S. Government from detecting and preventing the export of goods from the United States to Iran. IC Link Industries Ltd. ("IC Link") registered as a corporation in Ontario, Canada, and its office was located in the Toronto area. IC Link's business included procuring industrial goods in the United States for shipment to customers in Iran. IC Link's affiliate in Tehran, Iran was Sensor Co. Ltd. ("Sensor"). Sensor was responsible for coordinating IC Link's business with Iranian companies and handling IC Link's financial dealings in Iran. According to the indictment, it was part of the conspiracy that Shaneivar, through IC Link, received orders from Alamdari and others at Sensor on behalf of customers in Iran for industrial goods available in the United States. These orders were primarily for goods used in the oil, gas, petroleum, and energy industries. IC Link sent requests for quotes (RFQs) for the goods to an uncharged individual in the Northern District of Ohio, who obtained quotes from suppliers in the United States that he forwarded to IC Link. Typically, the goods were sent to the individual's business in the Northern District of Ohio. The goods were then shipped from the United States to an intermediary country other than Iran, such as the United Arab Emirates, Turkey, or other countries. Once the goods arrived in the intermediary country, a freight forwarder in that country re-shipped the goods to Iran. While in the intermediary country, the goods were sometimes re-packaged to disguise their origin in the United States. It was further part of the conspiracy that Shaneivar and IC Link sometimes used Mohamadi to arrange the shipment of goods procured in Ohio to the ultimate destination in Iran. Alamdari or Shaneivar provided information on the true destination of the goods in Iran to Mohamadi to arrange the shipment. When shipping goods on behalf of IC Link, Mohamadi typically used a shipping company in the United States to ship the goods from Ohio to Dubai, United Arab Emirates, and other transshipment locations. Once the goods were in Dubai or elsewhere, Mohamadi used a different freight forwarding company to re-ship the goods to Iran. On Sep. 10, 2019, Mohamadi pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act (IEEPA), and was sentenced to 24 months in prison.

Products for Pakistan Atomic Energy Commission - On June 1, 2017, in the District of Connecticut, Imran Khan, 43, of North Haven, waived his right to be indicted and pleaded guilty in federal court to violating U.S. export law. According to court documents and statements made in court, from at least 2012 to December 2016, Khan and others were engaged in a scheme to purchase goods that were controlled under the Export Administration Regulations (EAR) and export those goods without a license to Pakistan, in violation of the EAR. Khan conducted business as Brush Locker Tools or as Kauser Enterprises-USA. When asked by U.S. manufacturers about the end-user for a product, Khan either informed the manufacturer that the product would remain in the U.S., or he completed an end-user certification indicating that the product would not be exported. After the products were purchased, they were shipped by the manufacturer to Khan's North Haven residence or Cerda Market in New Haven, a business owned by Khan. The products were then shipped to Pakistan on behalf of either the Pakistan Atomic Energy Commission (PAEC), the Pakistan Space & Upper Atmosphere Research Commission (SUPARCO), or the National Institute of Lasers & Optronics (NILOP), all of which were listed on the U.S. Department of Commerce Entity List. Khan never obtained a license to export any item to a designated entity, even though he knew that a license was required prior to export. Khan pleaded guilty to one count of violating the International Emergency

Economic Powers Act. In pleading guilty, Khan specifically admitted that, between August 2012 and January 2013, he procured, received, and exported to PAEC an Alpha Duo Spectrometer without a license to do so. On September 19, 2018, Khan was sentenced by U.S. District Judge Stefan Underhill in Bridgeport to three years of probation, the first six months of which Khan must serve in home confinement. Judge Underhill also ordered Khan to perform 100 hours of community service and pay a $3,000 fine.

Dark Net Used to Export Firearms - In May 2017, in the Northern District of Georgia, Gerren Johnson and William Jackson were arraigned on federal charges of dealing in firearms without a license, smuggling goods from the United States to other countries, and illegal delivery of firearms to a common carrier. The defendants allegedly exported guns illegally to buyers all over the world. According to the charges and other information presented in court: In June 2013, the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and other agencies began investigating an international firearms trafficking scheme in which individuals utilized a Dark Net website called Blackmarket Reloaded (BMR). The individuals used the usernames CherryFlavor and WorldWide Arms. The investigation revealed that firearms posted for sale on this website were sold to persons outside the United States, and were shipped to buyers from the United States hidden inside electronic items. Some of the countries to which packages were shipped include Canada, the United Kingdom, and Australia. Federal search warrants, coupled with interviews, allegedly connected all firearms recovered from original purchasers in the Atlanta area to the defendants. The defendants had been acquiring firearms legally from the OutDoorTraders website, and later reselling the firearms on underground websites including BMR, Utopia, and Agora Market. Also, shipping information for over 50 suspected parcels was disseminated to investigators in Austria, Australia, Belgium, Canada, the United Kingdom, Ireland, Denmark, France, Germany, the Netherlands, and Sweden. Intelligence analysis, as well as a massive audit of internationally-shipped parcels originating from several suspect U.S. Post Offices, resulted in the identification of the individuals in the CherryFlavor group. Gerren Johnson, 28, of Austell, Georgia, was arraigned on May 24, 2017. William Jackson, 29, of East Point, Georgia, was arraigned on May 30, 2017. Two other defendants, Sherman Jackson and Brendan Person, previously were arrested and entered pleas of guilty. Sherman Jackson was sentenced to one year and nine months in prison, to be followed by two years of supervised release, after pleading guilty to smuggling firearms from the U.S. Brendan Person was sentenced to two years and three months in prison, to be followed by two years of supervised release, after pleading guilty to smuggling firearms from the U.S. On October 17, 2017, William Jackson pleaded guilty to smuggling goods from the U.S., and was sentenced to two years of probation. On January 9, 2018, Gerren Johnson pleaded guilty to smuggling firearms from the U.S., and was sentenced to two years and nine months in prison, to be followed by two years of supervised release.

Trade Secrets for Company in China - On May 24, 2017, in the District of Columbia, a criminal complaint was unsealed charging seven individuals with conspiring to steal trade secrets from a business in the United States on behalf of a company in China that was engaged in manufacturing a high-performance, naval-grade product for military and civilian uses. On May 23, 2017, two defendants were arrested in Washington, D.C., three in the Southern District of Texas, and one in the District of Massachusetts. All are charged in the U.S. District Court for the District of Columbia with conspiracy to commit theft of trade secrets. The government also filed a related civil forfeiture complaint in the District of Columbia for two pieces of real property which were involved in, and are traceable to, the alleged illegal conduct. Those arrested and charged include four U.S. citizens: Shan Shi, 52, of Houston, Texas; Uka Kalu Uche, 35, of Spring, Texas; Samuel Abotar Ogoe, 74, of Missouri City, Texas; and Johnny Wade Randall, 48, of Conroe, Texas. Also charged were Kui Bo, 40, a Canadian citizen who has been residing in Houston, and Gang Liu, 31, a Chinese national who has been residing in Houston as a permanent resident. Additionally, charges were filed against one Chinese national living in China, Hui Huang, 32, an employee of the Chinese manufacturing firm allegedly involved in tasking employees of the Houston company. According to an affidavit filed in support of the criminal complaint, the trade secrets were stolen in order to benefit a manufacturer located in China; this manufacturer was the only shareholder for a company that had been incorporated in Houston. Between

in or about 2012 and 2017, the affidavit alleges that the Chinese manufacturer and employees of its Houston-based company engaged in a systematic campaign to steal the trade secrets of a global engineering firm, referred to in the affidavit as "Company A," that was a leader in marine technology. The case involves the development of a technical product called syntactic foam – a strong, light material that can be tailored for commercial and military uses, such as oil exploration; aerospace; underwater vehicles, such as submarines; and stealth technology. According to the affidavit, the Chinese manufacturer intended to sell syntactic foam to both military and civilian, state-owned enterprises in China – part of a push toward meeting China's national goals of developing its marine engineering industry. The affidavit alleges that the conspirators took part in the theft of trade secrets from Company A, a multi-national company with a subsidiary in Houston that is among the major producers of syntactic foam. The affidavit identifies a number of trade secrets allegedly taken from the company between January and June of 2015, including secrets that allegedly were passed to people associated with the Chinese manufacturer and Houston-based company. This case is being investigated by the FBI's Houston Field Office; the U.S. Department of Commerce's Bureau of Industry and Security (BIS), Office of Export Enforcement; and the IRS-Criminal Investigation (IRS-CI). On April 26, 2018, Shan Shi and Gang Liu were charged by superseding indictment with conspiracy to commit economic espionage for the benefit of CBM-Future New Material Science and Technology Co. Ltd. (CBMF), a Chinese company based in Taizhou, China. Both businessmen were previously indicted in June 2017 for conspiracy to commit theft of trade secrets. The superseding indictment also charged CBMF and its Houston-based subsidiary, CBM International, Inc. (CBMI), for their roles in the conspiracy. The government reached plea agreements with Uka Kalu Uche, Samuel Abotar Ogoe, Johnny Wade Randall, and Kui Bo. On July 29, 2019, a trial jury found Shan Shi guilty of conspiracy to commit theft of trade secrets. Shan Shi is scheduled to be sentenced in January 2020.

Riflescopes for Russia - On May 10, 2017, in the Middle District of Pennsylvania, Mark Komoroski, age 54, of Nanticoke, Pennsylvania, was indicted for violating federal export laws and unlawfully possessing ammunition as a previously convicted felon. The indictment was unsealed on May 11, 2017, following Komoroski's arrest and initial appearance before United States Magistrate Judge Karoline Mehalchick. The indictment alleges that in February and March of 2016, Komoroski attempted to export two riflescopes to an individual in Russia without first obtaining the export licenses required by federal law. The indictment also alleges that Komoroski, a previously convicted felon, possessed over 25,000 rounds of ammunition. On January 16, 2018, Komoroski pleaded guilty to violating the International Emergency Economic Powers Act (IEEPA), but no sentencing date was set. This case was investigated by the Department of Homeland Security and the Department of Commerce.

Space Communications Technology to China - On May 23, 2017, in the Central District of California, Si Chen a/k/a Cathy Chen was arrested on federal charges of conspiring to procure and illegally export sensitive space communications technology to her native China. An indictment was returned by a federal grand jury on April 27, 2017, and was unsealed after Chen's arrest. The 14-count indictment accused Chen of violating IEEPA, which controls and restricts the export of certain goods and technology from the United States to foreign nations. Chen also was charged with conspiracy, money laundering, making false statements on an immigration application, and using a forged passport. According to the indictment, from March 2013 to December 2015, Chen purchased and smuggled sensitive items to China without obtaining licenses from the U.S. Department of Commerce that are required under IEEPA. Those items allegedly included components commonly used in military communications "jammers" from which Chen removed the export-control warning stickers prior to shipping. Additionally, Chen was suspected of smuggling communications devices worth more than $100,000 that are commonly used in space communications applications. On the shipping paperwork Chen falsely valued the items at $500. The indictment further described how Chen received payments for the illegally exported products through an account held at a bank in China by a family member. In July 2018, Chen pleaded guilty to conspiracy to violate the International Emergency Economic Powers Act (IEEPA); money laundering; and using a forged passport.

On Oct. 1, 2018, Chen was sentenced to 46 months in federal prison. The investigation in this case was conducted by U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI), the Department of Commerce's Office of Export Enforcement (OEE), and the Defense Criminal Investigative Service (DCIS).

Military Equipment Exported by Czech and Slovak Citizens - In May 2017, in the District of Connecticut, a federal grand jury in New Haven returned two indictments charging citizens of the Czech Republic and the Slovak Republic with offenses related to the illegal export of U.S. military equipment. On May 16, 2017, the grand jury returned a two-count indictment alleging that, between June 2011 and November 2011, Josef Zirnsak, 38, of the Czech Republic, shipped from the U.S. to Germany without a license an infrared dual beam aiming laser and a rifle scope, both of which are designated as defense articles on the U.S. Munitions List. On May 3, 2017, the grand jury returned a five-count indictment alleging that, between May 2012 and June 2012, Martin Gula, also known as "Mark Welder," 38, of the Slovak Republic, purchased and attempted to arrange, without a license, the export of night vision goggles and an aviator night vision system from the U.S. to the United Kingdom. This indictment also alleges that, during the same time period, Gula used a false U.S. passport as proof of residency and citizenship in the U.S. Zirnsak and Gula are each charged with two counts of violating the Arms Export Control Act. Gula also is charged with two counts of smuggling and one count of use of a false passport. Zirnsak and Gula are fugitives being sought by law enforcement. In January 2014, Gula was charged in the Central District of California with export related offenses. That indictment also is pending. This case is being investigated by the Defense Criminal Investigative Service (DCIS) and Homeland Security Investigations (HSI).

Night Vision Components to Russia - On April 27, 2017, in the Northern District of California, Naum Morgovsky and Irina Morgovsky were charged for their respective roles in an alleged scheme to export components for the production of night vision rifle scopes in violation of the Arms Export Control Act. The superseding indictment supplements bank fraud charges that were leveled in September 2016 against Naum Morgovsky and Mark Migdal. According to the superseding indictment, Naum and Irina Morgovsky owned night vision businesses in the United States and purchased numerous scope components including image intensifier tubes and lenses. The indictment alleges the Morgovskys conspired to ship these items to a night vision manufacturing company in Moscow, Russia, that was partly owned by Naum Morgovsky. The United States Munitions List prohibits export of these items unless the exporter obtains a license from the Department of State, Directorate of Defense Trade Controls. According to the indictment, the Morgovskys did not have such a license. In addition, the indictment alleges the Morgovskys took steps to conceal their crimes so that they could continue to run their illegal export business undetected. Naum Morgovsky laundered the proceeds of the export conspiracy, using a bank account in the name of a deceased person to conceal the ownership and control of the scheme's proceeds. The indictment further alleges that Irina Morgovsky used a passport that she fraudulently obtained in the name of another individual to travel to Russia three times in 2007. On June 12, 2018, Naum and Irina Morgovsky pleaded guilty for their respective roles in the scheme. Naum Morgovsky also pleaded guilty to laundering the proceeds of the scheme. In October 2018, Irina Morgovsky was sentenced to 18 months in prison. In November 2018, Naum Morgovsky was sentenced to 108 months in prison, assessed a fine of $1 million and assessed forfeiture of $222,929. The prosecution is the result of an investigation by the Federal Bureau of Investigation, Internal Revenue Service - Criminal Investigation, and the Department of Commerce.

Gun Parts Smuggled by Russian Citizen - On April 26, 2017, in the Northern District of Illinois, Konstantin Chekhovskoi, a citizen of the Russian Federation, was arrested on a complaint charging him with attempting to export articles from the United States contrary to U.S. law, in violation of 18 U.S.C. § 554. According to the complaint, U.S. Customs and Border Patrol (CBP) officers at O'Hare International Airport in Chicago selected Chekhovskoi for inspection pursuant to their border search authority as he attempted to board a commercial flight to Sweden. CBP inspected 11 suitcases, all of which were labeled

with airline baggage tags with Chekhovskoi's name on them. Among other things, officers uncovered rifle magazines and stocks, which they recognized to be enumerated on the U.S. Munitions List. Queries of appropriate law enforcement databases indicated Chekhovskoi did not have a license to export such items. In all, approximately 960 gun parts were seized from Chekhovskoi's luggage, including 196 magazines, 55 stocks, and 98 triggers. Chekhovskoi was taken into custody. A grand jury indicted him on July 27. On Dec. 12, 2017, Chekhovskoi pleaded guilty to smuggling. On March 22, 2018, he was sentenced to 18 months in federal prison and fined $100,000. This case was investigated by Homeland Security Investigations.

Conspiracy to Export U.S. Goods to Iran - On March 29, 2017, in the Western District of Washington, Ghobad Ghasempour, a Canadian citizen of Iranian descent, made his initial appearance in court after being charged with conspiracy to unlawfully export U.S.-origin goods to Iran, in violation of 18 U.S.C. § 371. Pursuant to an arrest warrant issued in the District of Columbia, Ghasempour was arrested on March 28 after crossing the U.S.-Canadian border in Blaine, Washington. According to the criminal complaint, beginning in December 2011, Ghasempour formed various front companies, based in China, to purchase U.S.-origin goods destined for Iranian end-users. In June 2015, Ghasempour's front company, Modo, transferred $150,000 to a company in Portugal with instructions that the money be used as a down payment for a "rate table" manufactured by Ideal Aerosmith, located in North Dakota. This machine is used to test and calibrate highly sophisticated navigation and sensor equipment of the type commonly found in military aircraft and missiles. Ghasempour and his co-conspirators intended this rate table for end use in Iran. In April 2018, Ghasempour pleaded guilty to conspiracy. On August 20, 2018, Ghasempour was sentenced to 42 months in prison. The case was investigated by Homeland Security Investigations.

Firearms to The Gambia - On March 27, 2017, in the Eastern District of North Carolina, Alhaji Boye was sentenced to 9 months of imprisonment followed by 3 years of supervised release. Boye pleaded guilty on October 31, 2016, to conspiracy to export defense articles (firearms) from the United States without a license. In 2012, with the intention of bringing political and social change to The Gambia, Gambian-American citizens and others joined a conspiracy entitled The Gambia Freedom League. The group hoped to take over the country, gain support from internal allies, and bring about regime change. The primary goal was to overthrow the Gambian President Yahya Jammeh, who had been in control of Gambia since his own coup in 1994 and whose rule had been marred by accusations of human rights violations. The conspiracy included directives for certain individuals to purchase firearms, others to ship them to The Gambia in 55-gallon barrels concealed among secondhand clothing, and others to travel and physically engage in the coup itself. Boye's role was to purchase firearms and ammunition. On December 30, 2014, members of the armed conspiracy attempted to violently breach the door of the State House in Gambia. The attempt failed and many of the conspirators died as a result of the ensuing gun battle. Following the assault, the Gambian military recovered at least 35 firearms, assault gear, vehicles, and 55-gallon barrels. On December 31, 2014, a member of The Gambia Freedom League returned to the United States and was interviewed by the Federal Bureau of Investigation (FBI). With the information received from the interview, the FBI initiated their investigation. The investigation revealed bank records displaying that on August 25, 2014, $7,000 had been wired to Boye in Raleigh, North Carolina. On August 26, 2014, Boye had purchased two AK-47 style assault rifles, as well as 7,000 rounds of ammunition, and 98 AK-47 magazines. On September 5, 2014, Boye also purchased four Diamondback rifles. In early 2015, following the failed coup, FBI agents traveled to The Gambia, inventoried and photographed the 35 firearms seized by the Gambian government. Five of those firearms matched serial numbers on the firearms purchased by Boye. This criminal investigation was conducted by the FBI and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

Hizballah Supporter Charged with Violating IEEPA - In March 2017, Kassim Tajideen, a prominent financial supporter of the Hizballah terror organization, was arrested and charged with evading U.S. sanctions imposed on him because of his financial support of Hizballah. Tajideen, 62, of Beirut, Lebanon,

was arrested overseas on March 12, 2017, based on an 11-count indictment unsealed in the U.S. District Court for the District of Columbia following Tajideen's arrival to the United States. Tajideen made his initial court appearance on March 24, 2017, before Magistrate Judge Robin M. Meriweather. The indictment charges Tajideen with one count of willfully conspiring to violate the International Emergency Economic Powers Act (IEEPA) and the Global Terrorism Sanctions Regulations, seven counts of unlawful transactions with a Specially Designated Global Terrorist, and one count of conspiracy to launder monetary instruments. The indictment also indicates that the government will seek a forfeiture money judgment equal to the value of any property, real or personal, which constitutes or is derived from proceeds traceable to these offenses. According to the indictment, Tajideen allegedly presided over a multi-billion-dollar commodity distribution business that operates primarily in the Middle East and Africa through a web of vertically integrated companies, partnerships, and trade names. The indictment further alleges that Tajideen and others engaged in an elaborate scheme to engage in business with U.S. companies while concealing Tajideen's involvement in those transactions. The Department of the Treasury's Office of Foreign Assets Control (OFAC) named Tajideen a Specially Designated Global Terrorist on May 27, 2009. This designation prohibits U.S. companies from transacting unlicensed business with Tajideen or any companies which are operated for his benefit – in essence stripping Tajideen's global business empire of its ability to legally acquire goods from, or wire money into, the United States. However, the indictment alleges that Tajideen restructured his business empire after the designation in order to evade the sanctions and continue conducting transactions with U.S. entities. Tajideen and others are alleged to have created new trade names and to have misrepresented his ownership in certain entities in order to conceal Tajideen's association. The scheme allowed Tajideen's companies to continue to illegally transact business directly with unwitting U.S. vendors, as well as to continue utilizing the U.S. financial and freight transportation systems to conduct wire transfers and move shipping containers despite the sanctions against Tajideen. According to the indictment, between approximately July of 2013 until the present day, the conspirators illegally completed at least 47 individual wire transfers, totaling over approximately $27 million, to parties in the U.S. During the same time period, the conspirators caused dozens of illegal shipments of goods to leave U.S. ports for the benefit of Tajideen, without obtaining the proper licenses from the Treasury Department. On December 6, 2018, Tajideen pleaded guilty before U.S. District Court Judge Reggie B. Walton to conspiracy to launder monetary instruments, in furtherance of violating the International Emergency Economic Powers Act (IEEPA). The plea called for an agreed-upon sentence of 60 months in prison. The plea agreement also required Tajideen to pay $50 million as a criminal forfeiture in advance of his sentencing. Tajideen has been detained since extradition to the United States in March 2017 after his arrest overseas. The arrest and indictment were the result of a two-year investigation led by the Drug Enforcement Administration (DEA) and assisted by U.S. Customs and Border Protection (CBP), as well as the Treasury Department's OFAC and Financial Crimes Enforcement Network.

Military-Grade Equipment to Ukraine – On March 7, 2017, in the Eastern District of New York, Volodymyr Nedoviz, a citizen of Ukraine and lawful permanent resident of the United States, was arrested on federal charges of illegally exporting controlled military technology from the United States to end-users in Ukraine in violation of the Arms Export Control Act (AECA) and the International Emergency Economic Powers Act (IEEPA). Federal agents also executed a search warrant at a Philadelphia, Pennsylvania location that was used in connection with Nedoviz's illegal scheme. The complaint alleges that Nedoviz conspired with others located in both Ukraine and the United States to purchase export-controlled, military-grade equipment from sellers in the United States and to export that equipment to Ukraine without the required export licenses from the U.S. Departments of Commerce or State. The devices obtained by the defendant and his co-conspirators included, among others, an Armasight Zeus-Pro 640 2-16x50 (60Hz) Thermal Imaging weapons sight, a FLIR Thermosight R-Series, Model RS64 60 mm 640x480 (30Hz) Rifle Scope, and an ATN X-Sight II 5-20x Smart Rifle Scope. In many cases, the devices purchased by Nedoviz and his co-conspirators retail for almost $9,000, and they are specifically marketed to military and law enforcement consumers. As part of the conspiracy, in order to induce U.S.-based manufacturers and suppliers to sell

them the export-controlled devices and to evade applicable export controls, the defendant and his co-conspirators falsely purported to be United States citizens and concealed the fact they were exporters. The defendant and his co-conspirators also recruited, trained, and paid other U.S.-based individuals to export the controlled devices to Ukraine via various freight forwarding companies. Among other things, the defendant and his co-conspirators instructed the U.S.-based individuals to falsely describe the nature and value of the equipment they were attempting to export. In addition, to conceal their identities, as well as the true destination of the rifle scopes and thermal imaging equipment, Nedoviz and his co-conspirators instructed that the items be shipped using false names and addresses. On July 18, 2017, Nedoviz pleaded guilty to one count of violating the AECA. On January 11, 2018, Nedoviz was sentenced to time served, 2 years supervised release, and forfeiture of $2,500. This case was investigated by the FBI.

Record Fine for Dual-Use Goods to Iran - On March 7, 2017, in the Northern District of Texas, ZTE Corporation agreed to enter a guilty plea and to pay a $430,488,798 fine and forfeiture penalty to the United States for conspiring to violate the International Emergency Economic Powers Act (IEEPA) by illegally shipping U.S.-origin items to Iran, obstructing justice, and making a material false statement. ZTE simultaneously reached settlement agreements with the U.S. Department of Commerce's Bureau of Industry and Security (BIS) and the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC). In total ZTE has agreed to pay the U.S. Government $892,360,064. The BIS has suspended an additional $300,000,000, which ZTE will pay if it violates its settlement agreement with the BIS. The plea agreement also required ZTE to submit to a three-year period of corporate probation, during which time an independent corporate compliance monitor will review and report on ZTE's export compliance program. ZTE is also required to cooperate fully with the Department of Justice (DOJ) regarding any criminal investigation by U.S. law enforcement authorities. The plea agreement ended a five-year joint investigation into ZTE's export practices, which was handled by DOJ's National Security Division, the U.S. Attorney's Office for the Northern District of Texas, the FBI, the BIS, and U.S. Immigration and Customs Enforcement's Homeland Security Investigations. A criminal information filed in federal court charged ZTE with one count of knowingly and willfully conspiring to violate the IEEPA, one count of obstruction of justice, and one count of making a material false statement. ZTE waived the requirement of being charged by way of federal indictment, agreed to the filing of the information, and accepted responsibility for its criminal conduct by entering into a plea agreement with the government. The plea agreement requires that ZTE pay a fine in the amount of $286,992,532 and a criminal forfeiture in the amount of $143,496,266. The criminal fine represents the largest criminal fine in connection with an IEEPA prosecution. According to documents filed in court, for a period of almost six years ZTE obtained U.S.-origin items – including controlled dual-use goods on the Department of Commerce's Commerce Control List (CCL) – incorporated some of those items into ZTE equipment and shipped the ZTE equipment and U.S.-origin items to customers in Iran. ZTE engaged in this conduct knowing that such shipments to Iran were illegal. ZTE further lied to federal investigators during the course of the investigation when it insisted, through outside and in-house counsel, that the company had stopped sending U.S.-origin items to Iran. In fact, while the investigation was ongoing, ZTE resumed its business with Iran and shipped millions of dollars' worth of U.S. items there.

Firearms Smuggled to Lebanon - On March 3, 2017, in the Northern District of Iowa, Fadi Yassine, age 42, a Lebanese citizen, was charged in a one-count Indictment with conspiring to violate the Arms Export Control Act (AECA) and to ship, transport, and deal firearms without a license. Yassine was arrested on February 5, 2017, in New York City as he entered the United States from Lebanon, pursuant to a warrant issued in the Northern District of Iowa on a criminal complaint charging him with conspiring to violate the AECA. He made an initial appearance in federal court in Cedar Rapids, Iowa, and was ordered detained without bond pending trial. According to allegations in the Indictment, Yassine conspired with others, including Ali Herz, to ship guns to Lebanon for resale there. The Indictment alleges that firearms were shipped to Lebanon from Cedar Rapids on about four occasions during 2014 and 2015. In April 2017,

Yassine pleaded guilty; in August 2017, he was sentenced to 57 months in prison. This case was investigated by Homeland Security Investigations; the Bureau of Alcohol, Tobacco, Firearms and Explosives; and the Federal Bureau of Investigation.

Firearms to Russia via Latvia - On Feb. 23, 2017, in the District of Connecticut, Michael Shapovalov a/k/a Mikhail Shapovalov was charged by complaint with violating the Arms Export Control Act (AECA), smuggling, conspiracy, false statements, and money laundering. Shapovalov is a Russian citizen and a legal permanent resident of the United States. The investigation of Shapovalov commenced as a result of an investigation conducted by the Federal Security Service (FSB) of the Russian Federation. In or about October 2015, the Department of Homeland Security, Homeland Security Investigations (DHS-HSI) in New Haven, Connecticut, received information from DHS-HSI in Moscow, Russia, indicating that firearms, firearm parts, and ammunition were being shipped from the United States to Latvia via the U.S. Postal Service (USPS). Once in Latvia, the packages were then being smuggled into Russia. The U.S. shipper of the parcels was identified as Shapovalov. The investigation revealed that since at least March 2015, Shapovalov acted as a United States-based intermediary and supplier for a co-conspirator in Latvia procuring firearms and firearm components, which are subject to U.S. export controls. The co-conspirator directed Shapovalov to make firearms purchases in the United States and ship the items via the USPS to Latvia, without an export license. When making these shipments, Shapovalov placed false descriptions of the items on the Air Waybills and/or the USPS shipping labels that accompanied the overseas packages, and failed to complete or submit any required export documents. The co-conspirator instructed Shapovalov as to which firearm parts he needed to acquire for Russian and Ukrainian customers by providing descriptions of items to purchase or, more often, providing a link to a website selling the specific item. Shapovalov, primarily using web-based distributors such as Gunbroker.com and eBay, purchased the requested items and had them shipped to his residence; he then repackaged the items and mailed them to addresses in Latvia. During the course of the investigation, more than 50 shipments to Latvia/Russia were identified as associated with Shapovalov. On Dec. 8, 2017, Michael Shapovalov pleaded guilty to a one-count Information charging him with exporting firearms parts without a license, in violation of the AECA. In May 2018, he was sentenced to 34 months in prison.

Gun Parts and Accessories to Thailand - On Feb. 16, 2017, in the District of Columbia, Pheerayuth Burden, 47, a Thai national who had been living in Torrance, California, was sentenced to 55 months in prison for taking part in a conspiracy involving the purchase and shipment of hundreds of gun parts and accessories from the United States to Thailand without a license. His company, Wing-On LLC, also was sentenced to three years of probation and ordered to pay a $250,000 fine. On Sep. 30, 2016, following a trial in the U.S. District Court for the District of Columbia, a jury found Burden and Wing-On LLC guilty of one count of conspiracy to violate the Arms Export Control Act and the International Traffic in Arms Regulations, one count of unlawful export of defense articles from the United States, and one count of conspiracy to commit money laundering. The Honorable Rosemary M. Collyer sentenced Burden and the company. Following his prison term, Burden will be placed on three years of supervised release. He and the company also were ordered to pay a forfeiture money judgment in the amount of $105,112. A co-defendant, Kitibordee Yindeear-Rom, 30, a native and citizen of Thailand, pleaded guilty to a conspiracy charge in November 2014. Yindeear-Rom was sentenced in March 2015 to a three-year prison term. According to the government's evidence, beginning at least in or about July 2010, Burden, Wing-On LLC, and Yindeear-Rom entered into an agreement to illegally ship United States origin goods, including defense articles - specifically gun parts - to Thailand. As part of their agreement, Yindeear-Rom purchased gun parts from United States manufacturers through on-line purchases, and directed the purchased items to be sent to Burden and Wing-On, which was based in Carson, California, to conceal the ultimate destination of the purchases. Upon receipt of the gun parts, the items would be repackaged for shipment to Thailand. Extending through at least October 2013 as part of the conspiracy, Burden and Yindeear-Rom caused to be purchased and shipped hundreds of different gun parts from the United States to Thailand without a license.

These gun parts included, for example, numerous firearm parts, including key components for AR-15 military-style assault rifles. The jury found that Burden and his company, Wing-On LLC, acted without a license and in knowing violation of federal export and money-laundering law. This case was investigated by Special Agents for U.S. Immigration and Customs Enforcement, Homeland Security Investigations, with assistance provided by the State Department's Directorate of Defense Trade Controls, U.S. Customs and Border Protection, and the U.S. Bureau of Alcohol, Tobacco, Firearms, and Explosives.

Defense Articles to China - On Feb. 15, 2017, in the Central District of California, Tian Min Wu a/k/a "Bob Wu," a citizen of the People's Republic of China (PRC), was charged in a six-count Indictment with purchasing and illegally exporting from the United States defense articles and items subject to the U.S. Munitions List (USML) and Commerce Control List (CCL) without an export license. According to the Indictment, Wu knowingly and willfully attempted to export from the United States a signals decoder – a defense article as defined in Category XI of the USML – without first having obtained a license or authorization for the Directorate of Defense Trade Controls (DDTC) of the U.S. Department of State. Category XI of the USML includes military electronics and software specifically designed for intelligence purposes. Wu also knowingly and willfully attempted to export from the United States to the PRC, intending to deliver it to the PRC Government, a satellite modem – a commercial good controlled by the CCL – without first having obtained a license or authorization from the U.S. Department Commerce. In February 2017, Tian Min Wu was arrested in Athens, Greece, under a provisional arrest warrant relating to charges contained in the Indictment. Subsequently, the U.S. Department of Justice requested Wu's extradition, and in December 2017 the Greek Court approved his extradition, pending final appeal. Wu was extradited to the United States in April 2018, and a trial was scheduled for November 2019.

Firearms Parts and Ammunition to the Philippines - On Feb. 15, 2017, in the Central District of California, a Long Beach woman pleaded guilty to federal offenses for illegally shipping tens of thousands of rounds of ammunition to the Philippines. Marlou Mendoza, 61, pleaded guilty in United States District Court to three counts of failing to provide the required written notice to freight forwarders that she was shipping ammunition to a foreign country. On June 19, 2017, she was sentenced to 2 years in prison. Marlou Medoza admitted that she sent .22-caliber ammunition and bullets to the Philippines in three shipments in June 2011. The shipments contained 131,300 rounds, the defendant admitted in court. In a related case unsealed in 2016, Mark Louie Mendoza, the 31-year-old son of Marlou Mendoza, was charged with illegally shipping hundreds of thousands of dollars' worth of firearms parts and ammunition to the Philippines – munitions that were concealed in shipments falsely claimed to be household goods. Mark Mendoza, who remains a fugitive, is named in an eight-count indictment that charges him with conspiracy, the unlawful export of munitions, smuggling and money laundering. Mark Mendoza, who was the president of a "tools and equipments" company known as Last Resort Armaments, ordered more than $100,000 worth of ammunition and firearms accessories, much of which was delivered to his parent's Long Beach residence over a six-month period in 2011. The items that Mark Mendoza ordered included parts for M-16 and AR-15-type rifles, and these parts are listed as defense articles on the United States Munitions List. Pursuant to the Arms Export Control Act, items on the Munitions List may not be shipped to the Philippines without an export license issued by the Department of State. The money laundering charge against Mark Mendoza alleges that during the first six months of 2011, Mark Mendoza transferred more than $650,000 in proceeds generated by the illegal ammunition exports from an account in the Philippines to a money remitter in Los Angeles. The charges against the Mendozas are the product of an investigation by U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).

Firearms on Hidden Internet Marketplace - On Jan. 30, 2017, in the District of Kansas, Michael Andrew Ryan was sentenced to 52 months in prison for his role in a scheme involving the illegal export of firearms from the United States using a hidden online marketplace. Michael Andrew Ryan, a/k/a Brad Jones and

GunRunner, 36, of Manhattan, Kansas, previously pleaded guilty to six counts of exporting and attempting to export firearms illegally from the United States to individuals located in other countries on June 6, 2016, and was remanded into custody on Oct. 6, 2016. In addition to the prison sentence, U.S. District Judge Daniel D. Crabtree ordered Ryan to forfeit all firearms and ammunition seized by law enforcement during the investigation. In connection with his plea, Ryan admitted that he used the hidden internet marketplace Black Market Reloaded, a website hosted on the Tor network where users can traffic anonymously in illegal drugs and other illegal goods, to unlawfully export or attempt to export dozens of firearms from the United States to Cork, Ireland; Mallow, Ireland; Pinner, England; Edinburgh, Scotland; and Victoria, Australia. These goods included pistols, revolvers, UZIs and Glocks, some from which the manufacturer's serial numbers had been removed, altered or obliterated, as well as magazines and hundreds of rounds of ammunition. The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) Kansas City Field Division investigated the case with assistance from ATF's National Investigative Division; U.S. Customs and Border Protection; U.S. Immigration and Customs Enforcement's Homeland Security Investigations; and the Manhattan and Riley County, Kansas, Police Departments.

Production and Development of Nuclear Material for China – On Jan. 6, 2017, in the Eastern District of Tennessee, Szuhsiung Ho, a/k/a Allen Ho, a naturalized U.S. citizen, pleaded guilty to conspiracy to unlawfully engage or participate in the production or development of special nuclear material outside the United States, without the required authorization from the U.S. Department of Energy (DOE), in violation of the Atomic Energy Act. On August 31, 2017, Ho was sentenced to 24 months in prison and fined $20,000. In April 2016, a federal grand jury issued a two-count indictment against Ho; China General Nuclear Power Company (CGNPC), the largest nuclear power company in China; and Energy Technology International (ETI), a Delaware corporation. At the time of the indictment Ho was a nuclear engineer, employed as a consultant by CGNPC, and was also the owner of ETI. CGNPC specialized in the development and manufacture of nuclear reactors and was controlled by China's State-Owned Assets Supervision and Administration Commission. According to documents filed in the case, beginning in 1997 and continuing through April 2016, Ho conspired with others to engage or participate in the development or production of special nuclear material in China, without specific authorization to do so from the U.S. Secretary of Energy, as required by law. Ho assisted CGNPC in procuring U.S.-based nuclear engineers to assist CGNPC and its subsidiaries with designing and manufacturing certain components for nuclear reactors more quickly by reducing the time and financial costs of research and development of nuclear technology. In particular, Ho sought technical assistance related to CGNPC's Small Modular Reactor Program; CGNPC's Advanced Fuel Assembly Program; CGNPC's Fixed In-Core Detector System; and verification and validation of nuclear reactor-related computer codes. Under the direction of CGNPC, Ho also identified, recruited, and executed contracts with U.S.-based experts from the civil nuclear industry who provided technical assistance related to the development and production of special nuclear material for CGNPC in China. Ho and CGNPC also facilitated travel to China for and payments to the U.S.-based experts in exchange for their services. This investigation was conducted by the FBI, Tennessee Valley Authority-Office of the Inspector General, DOE-National Nuclear Security Administration and U.S. Immigration and Customs Enforcement Homeland Security Investigations, with assistance from other agencies.

Munitions to Egypt – On Dec. 16, 2016, AMA United Group, Malak Neseem Swares Boulos and Amged Kamel Yonan Tawdraus were each sentenced in the Eastern District of New York after pleading guilty on April 1, 2015, to violating the Arms Export Control Act, in connection with the attempted shipment of munitions samples from New York City to Egypt. AMA United Group, an Egyptian procurement agent, entered a guilty plea to violating the Arms Export Control Act. Boulos and Tawdraus, Egyptian citizens and partners in AMA United Group, pleaded guilty to failing to file required export information relating to the international shipment of a landmine and multiple bomblet bodies. AMA United Group was sentenced to one year of probation and $400 special assessment. Boulos and Tawdraus were each sentenced to three years and six months home confinement, $100 special assessment and a fine of $2,500. According to court

filings and facts presented during the plea proceeding, Boulos and Tawdraus were arrested after attempting to close a deal to acquire and export the items, which were included on the U.S. Munitions List and regulated by the U.S. Department of State. Beginning in Feb. 2011, the defendants began trying to obtain munitions items on behalf of AMA United Group's client, a factory in Cairo. The items the defendants sought included a landmine as well as bomblet bodies and "trumpet liners," two components that are integral to manufacturing the housings for explosives in an aerial warhead. In July 2011, the defendants traveled from Cairo to New York City to inspect the items. On July 1, 2011, the three principals of AMA United Group attempted to ship samples to its client in Egypt. Boulos and Tawdraus failed to file any export information in connection with the attempted shipment. The requirement to file accurate information regarding the contents of international shipments is one layer of regulatory oversight pertaining to protecting the U.S. national security and diplomatic interests. This case was investigated by the U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI) and the Defense Criminal Investigative Service (DCIS).

Trade Secrets for Technologically Advanced Titanium to China – On Dec. 16, 2016, in the District of Connecticut, Yu Long, a citizen of China and lawful permanent resident of the U.S., waived his right to be indicted and pleaded guilty to charges related to his theft of numerous sensitive military program documents from United Technologies and transporting them to China. Long pleaded guilty to one count of conspiracy to engage in the theft of trade secrets knowing that the offense would benefit a foreign government, foreign instrumentality or foreign agent. He also pleaded guilty to one count of unlawful export and attempted export of defense articles from the U.S., in violation of the Arms Export Control Act. On June 27, 2017, Yu Long was sentenced to time served and a special assessment of $200. Previously, on Nov. 7, 2014, Long was arrested in Ithaca, NY, pursuant to a federal criminal complaint which charged Long with attempting to travel to China with sensitive proprietary documents that set forth detailed equations and test results used in the development of technologically advanced titanium for U.S. military aircraft. The documents were taken from a Connecticut defense contractor where Long had been employed. Long attempted, two days earlier, to fly to China from Newark Liberty International Airport in New Jersey. As alleged in the complaint affidavit and in statements made in court, Long holds Chinese citizenship and is a lawful permanent resident of the U.S. From approximately Aug. 2008, to May 2014, Long worked as a Senior Engineer/Scientist at a research and development center for a major defense contractor in Connecticut ("Company A"). Both during and after his employment there, Long traveled to the People's Republic of China. On Aug. 19, 2014, Long returned to the U.S. from China through John F. Kennedy International Airport in New York. During a secondary inspection screening by U.S. Customs and Border Protection (CBP) officers, Long was found in the possession of $10,000.00 in undeclared U.S. cash, registration documents for a new corporation being set up in China, and a largely completed application for work with a state-controlled aviation and aerospace research center in China. The application materials highlighted certain of Long's work history and experiences that he claimed to have obtained while employed at Company A, including work on F119 and F135 engines. The F119 engine is employed by the U.S. Air Force F-22 Raptor fighter aircraft. The F135 engine is employed by the U.S. Air Force F-35 Lightning II fighter aircraft. The criminal complaint and statements made in court further state that on Nov. 5, 2014, Long boarded a flight from Ithaca to Newark Liberty International Airport, with a final destination of China. During Long's layover in Newark, CBP officers inspected Long's checked baggage and discovered that it contained, among other things, sensitive, proprietary and export controlled documents from another major defense contractor located outside the state of Connecticut ("Company B"). Further investigation determined that the U.S. Air Force had convened a consortium of major defense contractors, including Company A and Company B, to work together to see whether they could collectively lower the costs of certain metals used. As part of those efforts, members of the consortium shared technical data, subject to stringent restrictions on further dissemination. Company B reviewed the Company B documents found in Long's possession at Newark Liberty Airport and confirmed that it provided the documents to Company A as part of the consortium. Company B further confirmed that Long was never an employee of Company B.

A review of Company A's computer records indicated that Long had printed the documents while employed at Company A. The documents bore warnings that they contained sensitive, proprietary and export-controlled material, which could not be copied or communicated to a third party. This investigation was conducted by the FBI, HSI, and CBP.

Prohibited Financial Transactions in Iran – On Dec. 15, 2016, in the District of Alaska, Kenneth Zong was named as the sole defendant in the 47-count indictment charging him with conspiracy to violate the International Emergency Economic Powers Act (IEEPA), unlawful provision of services to Iran, money laundering conspiracy and money laundering. The indictment alleged that at an undetermined time, Zong left Alaska for Seoul, South Korea, and operated businesses there. From January 2011 through at least April 2014, Zong and four co-conspirators – three Iranian nationals and one U.S. citizen – allegedly conspired to evade the prohibitions of IEEPA and Iranian Transactions and Sanctions Regulations (ITSR) by engaging in false and fraudulent transactions which were designed to unlawfully convert and remove Iranian owned funds, equivalent to approximately $1 billion United States dollars (USD). These funds were held in controlled Korean bank accounts and converted into more easily tradeable currencies, such as dollars and/or euros, by defrauding the Korean regulators into thinking the transactions were legitimate. Zong is charged with transferring those currencies to more than 10 countries around the world, including the U.S., United Arab Emirates, Switzerland, Germany, Austria and Italy. Zong received payment for these acts from the Iranian nationals in an amount from $10 million to $17 million USD. The indictment alleged that the scheme began in 2011, when Zong changed the name of his Korean company, "KSI Ejder, Inc." (KSI) to "Anchore." Zong used KSI/Anchore as a conduit to convert and distribute Iranian funds into USD and/or euros, by fictitiously selling marble tiles and other construction supplies to an Iranian shell company in Kish Island, Iran. KSI/Anchore fictitiously purchased Italian marble tiles and other construction supplies from "MSL & Co Investment Trading" (MSL Investment Dubai), an Iranian-controlled shell company in Dubai, which were then fictitiously shipped directly to another fictitious company in Iran. Zong and his co-conspirators created false and fictitious contracts, bills of lading and invoices to show Korean government banking regulators that the Iranian company owed KSI/Anchore for the false marble purchases. This resulted in the transfer of Iranian funds, at the direction of Zong's co-conspirators, from the restricted Iranian bank account to Zong's KSI/Anchore account. Zong then transferred the funds to entities and individuals throughout the world. Zong also is charged with 43 counts of money laundering and one count of money laundering conspiracy for his actions in connection with the $10 million fee paid to him by his Iranian associates. In furtherance of the scheme, Zong transferred $10 million of his fees from Korea to a co-conspirator who resided in Anchorage. This individual also created and operated various companies to be used as front companies to purchase real estate, automobiles, an interest in a yacht, and other purchases or transfers of the Iranian funds. The U.S. embargo on Iran, which is enforced through IEEPA and the ITSR, prohibits the export of goods, technology, and services to Iran with very limited exceptions. Zong is in custody in the Republic of South Korea for violations of Korean law. This case was investigated by the FBI and IRS-Criminal Investigation.

Components for IEDs to Iran and Iraq – On Dec. 15, 2016, in the District of Columbia, Lim Yong Nam, a/k/a Steven Lim, a citizen of Singapore, pleaded guilty to a federal charge stemming from his role in a conspiracy that allegedly caused thousands of radio frequency modules to be illegally exported from the U.S. to Iran. At least 16 of the components were later found in unexploded improvised explosive devices (IEDs) in Iraq. Lim was extradited from Indonesia, where he had been detained since Oct. 2014, in connection with the U.S. request for extradition. He pleaded guilty to a charge of conspiracy to defraud the U.S. by dishonest means. On April 27, 2017, Lim was sentenced to 40 months in prison. Lim and others were indicted in the District of Columbia in June 2010, on charges involving the shipment of radio frequency modules made by a Minnesota-based company. The modules have several commercial applications, including in wireless local area networks connecting printers and computers in office settings. These modules include encryption capabilities and have a range allowing them to transmit data wirelessly

as far as 40 miles when configured with a high-gain antenna. These same modules also have potentially lethal applications. Notably, during 2008 and 2009, coalition forces in Iraq recovered numerous modules made by the Minnesota firm that had been utilized as part of the remote detonation system for IEDs. According to the plea documents filed, between 2001 and 2007, IEDs were the major source of American combat casualties in Iraq. In his guilty plea, Lim admitted that between Aug. 2007, and Feb. 2008, he and others caused 6,000 modules to be purchased and illegally exported from the Minnesota-based company through Singapore, and later to Iran, in five shipments, knowing that the export of U.S.-origin goods to Iran was a violation of U.S. law. In each transaction, Lim and others made misrepresentations and false statements to the Minnesota firm that Singapore was the final destination of the goods. At no point in the series of transactions did Lim or any of his co-conspirators inform the company that the modules were destined for Iran. Similarly, according to the statement of offense, Lim and others caused false documents to be filed with the U.S. government, in which they claimed that Singapore was the ultimate destination of the modules. Lim and his co-conspirators were directly aware of the restrictions on sending U.S.-origin goods to Iran. Shortly after the modules arrived in Singapore, they were kept in storage at a freight forwarding company until being aggregated with other electronic components and shipped to Iran. There is no indication that Lim or any of his co-conspirators ever took physical possession of these modules before they reached Iran or that they were incorporated into another product before being re-exported to Iran. According to the statement of offense, 14 of the 6,000 modules the defendants routed from Minnesota to Iran were later recovered in Iraq, where the modules were being used as part of IED remote detonation systems. This investigation was jointly conducted by ICE Homeland Security Investigations (HSI) and the Department of Commerce, Bureau of Industry and Security. Substantial assistance was provided by the U.S. Department of Defense, U.S. Customs and Border Protection, the State Department's Directorate of Defense Trade Controls, the Treasury Department's Office of Foreign Assets Control, and the Office of International Affairs in the Justice Department's Criminal Division, the Justice Department Attaché in the Philippines and the FBI and HSI Attachés in Singapore and Jakarta.

Aviation Parts and Supplies to Iran – On Dec. 14, 2016, in the District of Columbia, Mansour Moghtaderi Zadeh, an Iranian national, was sentenced to 18 months in prison and one year of supervised release for taking part in a conspiracy involving the purchase and shipment of various products, including aviation parts and aviation supplies, from the U.S. to Iran without a license. Zadeh was also ordered to pay a forfeiture money judgment in the amount of $69,159.00. Zadeh, who had been living in Iran, pleaded guilty on Oct. 27, 2016, to one count of conspiracy to unlawfully export goods, technology and services to Iran without the required license, and to defraud the U.S., in violation of 18 U.S.C. § 371, 50 U.S.C. § 1705, and 31 C.F.R. Parts 560.203 and 560.204. In court documents filed at the time of the plea, Zadeh acknowledged that beginning in Oct. 2005, Iranian companies requested that Zadeh through his company, Barsan, procure products including a fiber optic video transmitter and receiver, and aviation course indicators that would otherwise require a license from the Office of Foreign Assets Control (OFAC) to be exported to Iran. Members of the conspiracy arranged for the items to be sent from the U.S. to Iran, for which Zadeh received a commission. In March 2007, Zadeh and co-conspirators attempted to export metal sheets and rods that are used in the aviation manufacturing industry from the U.S. to Iran without the required license from OFAC. Zadeh had arranged for his new corporation, Lavantia, to purchase the items. Zadeh also used an alias in his communications. In Sep. 2007, the shipment was detained by the U.S. Department of Commerce pending certification of the end user. In Oct. 2007, the Department of Commerce issued a Temporary Denial Order (TDO) against Lavantia and Zadeh, under his alias. The TDO prohibited Lavantia and Zadeh from participating in any way in exporting commodities from the U.S. Notwithstanding the TDO, Zadeh and other conspirators exported and attempted to export numerous materials from the U.S., including resin, sealant, paint, pneumatic grease, film adhesive and polyurethane coating and thinner. The post-TDO conduct included more than $69,000 of exported goods. This investigation was conducted by the U.S. Immigration and Customs Enforcement's Homeland Security Investigations, and the Bureau of Industry and Security at the U.S. Department of Commerce.

Cutting-Edge Microelectronics to Russia – On Dec. 6, 2016, in the Eastern District of New York, Alexey Barysheff of Brooklyn, New York, a naturalized citizen of the United States, was arrested on federal charges of illegally exporting controlled technology from the United States to end-users in Russia. Simultaneously, two Russian nationals, Dmitri Aleksandrovich Karpenko and Alexey Krutilin, were arrested in Denver, Colorado, on charges of conspiring with Barysheff and others in the scheme. Federal agents also executed search warrants at two Brooklyn locations that were allegedly used as front companies in Barysheff's illegal scheme. Barysheff made his initial appearance on Dec. 6, 2016, in the Eastern District of New York. Karpenko and Krutilin made their initial appearances on Dec. 6, 2016, in the District of Colorado. On Dec. 18, 2016, the Court ordered their removal in custody to the Eastern District of New York. The complaints allege that Barysheff, Karpenko, Krutilin, and others were involved in a conspiracy to obtain cutting-edge microelectronics from manufacturers and suppliers located within the United States and to export those high-tech products to Russia, while evading the government licensing system set up to control such exports. The microelectronics shipped to Russia included, among other products, digital-to-analog converters and integrated circuits, which are frequently used in a wide range of military systems, including radar and surveillance systems, missile guidance systems and satellites. These electronic devices required a license from the Department of Commerce to be exported to Russia and have been restricted for anti-terrorism and national security reasons. As further detailed in the complaints, in 2015 Barysheff registered the Brooklyn, New York-based companies BKLN Spectra, Inc. (Spectra) and UIP Techno Corp. (UIP Techno). Since that time, the defendants and others have used those entities as U.S.-based front companies to purchase, attempt to purchase, and illegally export controlled technology. To induce U.S.-based manufacturers and suppliers to sell them high-tech, export-controlled microelectronics and to evade applicable controls, the defendants and their co-conspirators purported to be employees and representatives of Spectra and UIP Techno and provided false end-user information in connection with the purchase of the items, concealed the fact that they were exporters and falsely classified the goods they exported on records submitted to the Department of Commerce. To conceal the true destination of the controlled microelectronics from the U.S. suppliers, the defendants and their co-conspirators shipped the items first to Finland and subsequently to Russia. On March 2, 2017, Barysheff pleaded guilty to submitting false export information; on Oct. 19, 2017, Barysheff was sentenced to time served. Karpenko and Krutilin pleaded guilty to conspiracy to violate IEEPA; they were sentenced to time served and were ordered removed from the United States on May 2, 2017. This case was investigated by ICE-HSI, FBI, Department of Commerce-BIS, and DoD DCIS.

Controlled Microelectronics to Russian Military and Intelligence Agencies – On Dec. 1, 2016, Shavkat Abdullaev was sentenced in the Eastern District of New York to 36 months' imprisonment, 2 years supervised release, and a $400 special assessment. On Feb. 28, 2017, Alexander Posobilov was sentenced to 135 months in prison. Previously, on July 21, 2016, Alexander Fishenko, a dual citizen of the United States and Russia, was sentenced to 120 months' imprisonment and ordered to forfeit more than $500,000 in criminal proceeds following his guilty plea on Sep. 9, 2015, to a nineteen-count indictment. Fishenko was charged with acting as an agent of the Russian government within the United States without prior notification to the Attorney General, conspiring to export, and illegally exporting controlled microelectronics to Russia, conspiring to launder money, and obstruction of justice. Fishenko, ten other individuals, and two corporations – ARC Electronics, Inc. (ARC) and Apex System, L.L.C. (Apex) – were indicted in Oct. 2012. On Oct. 26, 2015, Alexander Posobilov, Shavkat Abdullaev and Anastasia Diatlova were convicted of all counts of the indictment. On Jan. 10, 2013, defendants Lyudmila Bagdikian and Viktoria Klebanova pleaded guilty for their roles in exporting goods from the United States to Russian end users. Three defendants remain at large. ARC is now defunct, and Apex, a Russian-based procurement firm, failed to appear in court. Previously, on Oct. 3, 2012, an indictment was unsealed in the Eastern District of New York charging 11 members of a Russian procurement network operating in the United States and Russia, as well as a Houston-based export company, Arc Electronics Inc., and a Moscow-based procurement firm, Apex System L.L.C., with illegally exporting high-tech microelectronics from the United

States to Russian military and intelligence agencies. Fishenko, an owner and executive of both the American and Russian companies, was also charged with operating as an unregistered agent of the Russian government inside the U.S. by illegally procuring the microelectronics on behalf of the Russian government. The microelectronics allegedly exported to Russia are subject to U.S. controls due to their potential use in a wide range of military systems, including radar and surveillance systems, weapons guidance systems and detonation triggers. In conjunction with the unsealing of the charges, the Department of Commerce added 165 foreign persons and companies who received, transshipped, or otherwise facilitated the export of controlled commodities by the defendants to its "Entity List." As alleged in the indictment, between Oct. 2008, and the present, Fishenko and the other defendants engaged in a conspiracy to obtain advanced microelectronics from manufacturers and suppliers located in the United States and to export those high-tech goods to Russia, while evading the government export licensing system. The microelectronics shipped to Russia included analog-to-digital converters, static random access memory chips, microcontrollers and microprocessors. The defendants allegedly exported many of these goods, frequently through intermediary procurement firms, to Russian end users, including Russian military and intelligence agencies, and went to great lengths to conceal their procurement activities. The investigation uncovered a Russian Ministry of Defense document designating an Apex subsidiary as a company "certified" to procure and deliver military equipment and electronics. The FBI recovered a letter sent by a specialized electronics laboratory of Russia's Federal Security Service (FSB), Russia's primary domestic intelligence agency, to an Apex affiliate regarding certain microchips obtained for the FSB by Arc. The defendants' principal port of export for these goods was John F. Kennedy International Airport in New York. In addition to Fishenko, Arc, Apex, Posobilov, Abdullaev and Diatlova, the indictment also charged Sevinj Taghiyeva and Svetalina Zagon, who were arrested in Houston on Oct. 2 and Oct 3, 2012. Three others charged in the indictment, Sergey Klinov, Yuri Savin, and Dimitriy Shegurov, were based overseas and were not arrested. The investigation was conducted by the FBI, Department of Commerce (BIS), Naval Criminal Investigative Service (NCIS) and the IRS.

Assault Rifles to Haiti – On Dec. 1, 2016, an indictment was returned in the Southern District of Florida charging both Samuel Baptiste and Jose Noel a/k/a Abdul Jabar, a citizen of Haiti, with smuggling goods from the United States. The indictment also charged Noel with being an alien in possession of a firearm and Baptiste with being a felon in possession of a firearm. The investigation of Baptiste began in April 2014, when investigating agents observed that Baptiste operated numerous social media accounts praising U.S. designated terrorists Usama bin Laden and Anwar Al-Awlaki, in addition to encouraging jihad and referencing becoming a martyr. The FBI assessed that Baptiste used his social media accounts since at least 2013 to disseminate extremist propaganda, to praise attacks conducted or inspired by Al Qaeda, and to promote travel to Syria for jihad. In mid-Oct. 2016, FBI agents launched an investigation of Noel based on information provided by a FBI Confidential Human Source (CHS). The CHS was first introduced to Noel through a mutual associate, Baptiste, in Oct. 2016. During a meeting between Baptiste, Noel and the CHS, Noel indicated a desire to obtain a T-56 rifle. Noel stated that he had previously obtained illegal guns from family members in Florida and further claimed to have transported concealed weapons to Haiti in the past. Noel also told the CHS about a security company he was trying to establish in Haiti and his desire to obtain guns for this company. During one of the meetings between the CHS, Baptiste and Noel, Noel advised the CHS that he (Noel) needed a 9mm handgun and also wanted to purchase an AR-15 assault rifle. On Nov. 5, 2016, Baptiste, Noel and the FBI CHS went to a shipping container acquired by the CHS. The CHS told Baptiste and Noel that the container was scheduled to be shipped to Haiti. Inside the container were FBI-acquired items that resembled relief items to be shipped to Haiti. Among the items were pallets of food, clothing, vehicle tires, and household appliances. Also placed inside the container concealed under clothing were two FBI-provided rifles – two Rock River Arms LAR-15 semi-automatic assault rifles – and four ammunition magazines for those rifles. The weapons were provided to Noel based on his requests to the FBI CHS to obtain AR-15-style rifles for him. Noel paid the CHS $300 in case for one of the weapons. On March 30, 2017, Noel pleaded guilty to being an alien in possession of a firearm; on May 30, 2017, he was

sentenced to 16 months in prison. On March 31, 2017, Baptiste pleaded guilty to being a felon in possession of a firearm; on June 21, 2017, he was sentenced to 80 months in prison. This case was investigated by the FBI.

Sanctions Violations to Aid Iran – On Nov. 21, 2016, in the Eastern District of New York, Ahmad Sheikhzadeh, a U.S. citizen and resident of New York City, pleaded guilty to filing a false income tax return that substantially understated the amount of cash salary the defendant received from Iran's Permanent Mission to the United Nations (IMUN) and conspiring to facilitate the transfer of funds to Iran without the required license from the Treasury Department, in violation of the International Emergency Economic Powers Act (IEEPA). According to court filings and facts presented during the plea proceeding, beginning in Jan. 2008, Sheikhzadeh was employed as a consultant to the IMUN and received a regular salary, in cash, approximately once per month, through an intermediary who was an official at the IMUN. Sheikhzadeh was not a declared IMUN official. From 2008 through 2012, Sheikhzadeh filed personal income tax returns that substantially understated the amount of income he received from his work for the IMUN. In addition, distinct from his work for the IMUN, Sheikhzadeh provided money remitting ("hawala") services to co-conspirators in the U.S. to facilitate investments in Iran and to direct disbursements from Iranian bank accounts. Sheikhzadeh engaged in these money transfers without a license from the Treasury Department's Office of Foreign Assets Control, in violation of IEEPA. The defendant agreed to pay over $147,000 in restitution and forfeiture. In February 2018, Sheikhzadeh was sentenced to 3 months in prison and fined $10,000. This case is investigated by the FBI and the IRS Criminal Investigation Division in New York.

Integrated Circuits to China – On Nov. 4, 2016, in the District of Connecticut, Xianfeng Zuo of Shenzhen, China, was sentenced to 15 months of imprisonment for conspiring to sell counterfeits of sophisticated integrated circuits (ICs) to a purchaser in the U.S. According to court documents and statements made in court, Zuo, Jiang Yan and Daofu Zhang each operated businesses in China that bought and sold electronic components, including ICs. In the summer of 2015, Zuo asked Yan to locate and purchase several advanced ICs made by Xilinx Corp., which had military applications, including radiation tolerance for uses in space. Yan then asked a U.S. individual to locate the Xilinx ICs and sell them to Yan. The U.S. individual explained that the ICs cannot be shipped outside the U.S. without an export license, but Yan still wished to make the purchase. When the U.S. individual expressed concern that the desired ICs would have to be stolen from military inventory, Yan proposed to supply the U.S. source with "fake" ICs that "look the same," to replace the ones to be stolen from the military. In Nov. 2015, Zhang shipped from China to the U.S. individual, two packages containing a total of eight counterfeit ICs, each bearing a counterfeit Xilinx brand label. After further discussions between Yan and the U.S. individual, Yan, Zhang, and Zuo flew together from China to the U.S. in early Dec. 2015, to complete the Xilinx ICs purchase. On Dec. 10, 2015, the three conspirators drove to a location near Route 95 in Milford, Connecticut, where they planned to meet the U.S. individual, make payment, and take custody of the Xilinx ICs. Federal agents arrested all three at the meeting location. The defendants were charged under separate indictments in the District of Connecticut. On March 7, 2016, Yan pleaded guilty both to conspiracy to traffic in counterfeit military equipment, in violation of 18 U.S.C. § 2320(a)(3); and to attempted, unlicensed export of advanced, export-restricted electronic equipment, in violation of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701 et seq. Yan was sentenced on Dec. 29, 2016, to time–served. On March 16, 2016, Zuo pleaded guilty to one count of conspiracy to traffic in counterfeit goods, in violation of 18 U.S.C. § 2320(a). On April 15, 2016, Zhang also pleaded guilty to one count of conspiracy to traffic in counterfeit goods. Zhang was sentenced on July 8, 2016, to 15 months of imprisonment. As part of their sentences, each defendant was ordered to forfeit his interest in the $63,000 in cash seized incident to their arrests. This matter was investigated by the Defense Criminal Investigative Service, the Department of Homeland Security, the Department of Commerce, the Federal Bureau of Investigation, and the Air Force Office of Special Investigations.

Firearm Parts to the Philippines – On Nov. 2, 2016, Kirby Santos of the Republic of the Philippines was sentenced in the District of New Jersey to 24 months' imprisonment, 3 years supervised release, $100 special assessment and $2,400 fine after pleading guilty on Oct. 7, 2015, to an information charging him with one count of conspiracy to violate the Arms Export Control Act and U.S. anti-smuggling laws. According to the documents filed in this case, other cases and statements made in court: Santos admitted that from 2008 through Oct. 2013, he and conspirators he met in the Philippines or through an online forum agreed to ship firearms parts from the United States to the Philippines. Santos and others used credit cards and other forms of payment to purchase firearms parts from suppliers in the United States. Knowing that they would not ship to the Philippines, Santos arranged for the suppliers to send the firearms parts to the addresses of conspirators in Toms River, New Jersey, and Lynwood, Washington, in order to make the purchases appear as domestic sales. At the direction of Santos, the conspirators, including Abelardo Delmundo, 53, of Toms River, New Jersey, would then repackage the firearms parts, falsely label the contents of the package and export the firearms parts to the Philippines for ultimate delivery to Santos. To disguise their role in the conspiracy, the conspirators used aliases when sending the packages containing prohibited items. Upon receiving the firearms parts, Santos paid Delmundo and other conspirators in the form of cash or wire transfers to others at their direction. During the course of the nearly five-year long conspiracy, Santos and others purchased and directed the unlawful exportation of more than $200,000 worth of defense articles from the United States to the Philippines without the required export license. Santos made his initial appearance in federal court on April 22, 2015, after being charged by criminal complaint with one count of conspiracy to violate the Arms Export Control Act and U.S. anti-smuggling laws. The Arms Export Control Act prohibits the export of defense articles and defense services without first obtaining a license from the U.S. Department of State and is one of the principal export control laws in the United States. Santos was arrested in Guam on March 31, 2015, by special agents of the U.S. Department of Homeland Security-Homeland Security Investigations (DHS-HSI) and the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). Delmundo, charged in the District of New Jersey under a separate information, pleaded guilty to his role in the conspiracy on April 30, 2015. This investigation was conducted by DHS-HSI, ATF.

Firearms and Ammunition to Ghana – On Nov. 2, 2016, in the Western District of North Carolina, Richmond Akoto Attah was sentenced to 37 months of imprisonment, one year supervised release, and $100 special assessment stemming from his plea of guilty on June 7, 2016, to smuggling goods from the United States. On Feb. 16, 2016, a nine count indictment was returned charging Attah with one count of violating the Arms Export Control Act (AECA), one count of illegal firearms dealing, two counts of smuggling goods from the United States and four counts of making false statements to a firearms dealer. According to the indictment, beginning in at least 2013, Attah purchased numerous firearms and ammunition he intended to smuggle and illegally export to Ghana, West Africa. Attah obtained the firearms by misstating on the required federal forms that he was the actual buyer and transferee of the firearms. According to the indictment, Attah was not a federally licensed firearms dealer and did not possess a license to export firearms or ammunition to Ghana or any other country. The indictment further alleged that from on or about Sep. 2013, to Dec. 2015, Attah purchased approximately 63 firearms and 3,500 rounds of ammunition from various stores, internet vendors and at gun shows. On or about Sep. 4, 2015, Attah travelled from Charlotte to Ghana, returning on Oct. 10, 2015. During his return trip, Attah hid $30,100 dollars in his luggage, falsely declaring on his customs paperwork that he was only bringing $350 back into the United States. The indictment also alleged that from on or about Nov. 2015, to Dec. 13, 2015, Attah purchased approximately 22 firearms and ammunition from dealers in North Carolina and online. Attah then hid 27 firearms, including semi-automatic pistols and revolvers, inside a washing machine and a dryer, and 3,500 rounds of ammunition inside a barrel. Attah placed the washer, dryer, and barrel inside a shipping container and attempted to have it shipped from Charlotte to Ghana. According to court documents, U.S. Customs officers recovered the firearms and ammunition before they were shipped outside the United States. This case was investigated by ATF, FBI, ICE HSI and CBP.

Military Aircraft Parts to Iran – On Oct. 26, 2016, in the Central District of California, a nine-count federal indictment was unsealed charging five defendants in a scheme to smuggle millions of dollars' worth of military aircraft parts and other potential defense items to Iran, in violation of the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR). Zavik Zargarian and Vache Nayirian were arrested on federal charges for their alleged roles in the scheme and were taken into custody by special agents of U.S. Immigration and Customs Enforcement's HSI. The men allegedly were part of a conspiracy to purchase and ship more than $3 million dollars' worth of jet fighter aircraft parts to Iran. Additionally, several of the defendants were accused of buying and illegally exporting fluorocarbon rubber O-rings to Iran. The O-rings in question have a variety of possible military applications, including use in aircraft hydraulic systems and landing gear. Also named in the indictment are Zargarian's Glendale-based company, ZNC Engineering, and two Iranian nationals, Hanri Terminassian, and Hormoz Nowrouz, both of whom are believed to be in Iran. The charges stem from a lengthy undercover probe spearheaded by HSI, with substantial assistance provided by the Defense Criminal Investigative Service and U.S. Customs and Border Protection (CBP). According to the indictment, Terminassian originally contacted Zargarian from Iran for assistance with obtaining military aircraft parts from U.S.-based suppliers. Subsequently, Zargarian negotiated on Terminassian's behalf to purchase the desired items from an undercover HSI special agent who was posing as a parts supplier. The items included parts used in F-14, F-15, F-16 and F-18 fighter jets. Eventually, Terminassian traveled to the U.S. to meet with Zargarian and the undercover special agent to discuss the transaction. The indictment alleged the two men sought to purchase between 10 and 30 units of each item, with the total cost potentially exceeding $3.6 million. The indictment also accuses Zargarian and Nayirian of conspiring with Terminassian and Nowrouz to export fluorocarbon rubber O-rings to Iran. The indictment alleged Terminassian contacted Nayirian and Zargarian on behalf of Nowrouz and sought their help to obtain the parts. Terminassian transferred funds for the purchase to Nayirian, who later provided the money to Zargarian. Through his company ZNC Engineering, Zargarian bought the O-rings from a California vendor and provided them to Nayirian. Nayirian then exported the O-rings to addresses in the United Arab Emirates and Kuwait provided by Terminassian, who subsequently arranged for them to be transshipped to Iran. According to the indictment, the defendants exported more than 7,000 O-rings to Iran over the course of the conspiracy. To reduce the likelihood of detection, the defendants falsely claimed on shipping documents that the O-rings were destined for countries other than Iran and substantially undervalued them to avoid having to file export forms that might prompt further inspection by CBP. As part of their probe, investigators obtained evidence that the O-rings were intended for the Iranian Air Force. Zargarian and Nayirian were arraigned on the indictment in federal court on Oct. 26, 2016. Both men entered not guilty pleas. On April 17, 2017, Zargarian pleaded guilty to conspiracy to violate IEEPA, and later was sentenced to 41 months in prison. The indictment against Nayirian was dismissed. This case was investigated by ICE-HSI.

Proprietary Rice Seeds to China – On Oct. 26, 2016, in the District of Kansas, Wengui Yan pleaded guilty to one count of making false statements to the FBI while working as a geneticist for the U.S. Department of Agriculture at the Dale Bumpers National Research Center in Stuttgart, Arkansas. Yan, a scientist who worked with rice, admitted that he knew about plans to steal samples and send them to China. In his plea, Yan admitted that on Aug. 7, 2013, agents of U.S. Customs and Border Protection found stolen seeds in the luggage of a group of visitors from China preparing to board a plane to return home. The group had visited the facility in Stuttgart. Yan admitted that before the Chinese group arrived, a co-defendant in Kansas had asked him for seeds and Yan had declined because the seeds were protected. The co-defendant told Yan about other individuals seeking to steal samples of the seeds. When the delegation came to Stuttgart, Yan traveled with them to a rice farm where he knew they would have an opportunity to steal seeds. After the theft, Yan denied knowing about the plans to steal the seeds or about the theft itself. Investigators also learned that Yan attempted to cover up a trip he made to China to visit the crops research institute that sent the delegation to the United States. In February 2017, co-defendant Weiqiang Zhang was convicted at trial

of conspiracy to steal trade secrets and interstate transportation of stolen property. On April 4, 2018, Zhang was sentenced to 121 months in prison; on July 31, 2018, Yan was sentenced to 13 months in prison. This case was investigated by the FBI and CBP.

Restricted Laboratory Equipment to Syria – On Oct. 25, 2016, in the Middle District of Pennsylvania, Ahmad Feras Diri of London, United Kingdom, was sentenced to 37 months' imprisonment and $100 special assessment after pleading guilty on April 21, 2016, to conspiracy to export items from the United States. Diri will be deported once he has completed his sentence. On Oct. 13, 2016, Harold Rinko, a U.S. citizen, was sentenced to time served, 2 years supervised release, $100 special assessment and a fine of $2500, after pleading guilty on Sep. 16, 2014, to conspiracy to export items from the United States. Rinko is also required to wear an electronic monitor for twelve months. Previously, on Nov. 20, 2012, an indictment was returned in the Middle District of Pennsylvania charging Diri; Mowea Diri, Ahmad's brother and a citizen of Syria; d-Deri Contracting & Trading, a business located in Syria; and Rinko with criminal conspiracy, wire fraud, illegal export of goods, money laundering and false statements. On March 14, 2013, Diri was arrested by the Metropolitan Police in London in connection with the charges in the indictment and was extradited to the United States by the United Kingdom on Nov. 12, 2015. Diri was arraigned on charges alleging a conspiracy to illegally export laboratory equipment, including items used to detect chemical warfare agents, from the United States to Syria. The indictment alleged that from 2003 until Nov. 20, 2012, the three men conspired to export items from the United States through third party countries to customers in Syria without the required U.S. Commerce Department licenses. According to the indictment, the conspirators prepared false invoices that undervalued and mislabeled the goods being purchased and listed false information regarding the buyers' identity and geographic location. The indictment alleged that the items were to be shipped from the United States to Jordan, the United Arab Emirates and the United Kingdom, and thereafter transshipped to Syria. The indictment further states that the items allegedly included: a portable gas scanner used for detection of chemical warfare agents by civil defense, military, police and border control agencies; a handheld instrument for field detection and classification of chemical warfare agents and toxic industrial chemicals; a laboratory source for detection of chemical warfare agents and toxic industrial chemicals in research, public safety and industrial environments; a rubber mask for civil defense against chemicals and gases; a meter used to measure chemicals and their composition; flowmeters for measuring gas streams; a stirrer for mixing and testing liquid chemical compounds; industrial engines for use in oil and gas field operations; and a device used to accurately locate buried pipelines. Pursuant to regulations of the U.S. Department of Commerce's Export Administration, a license is required to export goods and services from the United States to Syria, excepting limited and certain categories of humanitarian food and medicine. This case was investigated by ICE-HSI and U.S. Commerce Department's Office of Export Enforcement.

Firearm Parts to Republic of Turkey – On Oct. 7, 2016, Hamza Kolsuz, a citizen of the Republic of Turkey, was sentenced in the Eastern District of Virginia to 30 months' imprisonment, 3 years supervised release and ordered to pay $200 special assessment. Previously, on June 24, 2016, the Court issued Findings of Fact and Conclusions of Law finding Kolsuz guilty of all three counts in the indictment pending against him. The Court's ruling followed a two-day bench trial on May 18-19, 2016. On March 2, 2016, after having previously been charged in a Criminal Complaint, a grand jury in the Eastern District of Virginia returned a three-count indictment against Kolsuz, charging him with: (1) conspiring to violate the Arms Export Control Act (the AECA) and 18 U.S.C. § 554(a), in violation of 18 U.S.C. § 371; (2) attempting to export defense articles on the United States Munitions List (USML) without a license or other written authorization from the United States Department of State's Directorate of Defense Trade Controls (the DDTC), in violation of the AECA; and (3) attempting to smuggle goods out of the United States, in violation of 18 U.S.C. § 554(a). The charges stemmed from Kolsuz's attempt to export firearms parts—specifically, eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, one .357 caliber handgun magazine and one .22 caliber Glock caliber conversion kit—to the Republic of

Turkey, and his involvement in a years-long conspiracy to export firearms parts to the Republic of Turkey. Kolsuz arrived in the United States at Miami International Airport on Jan. 25, 2016, on a B-2 visitor's visa. While in Florida, Kolsuz and one of his co-conspirators visited gun stores and a gun show where they purchased firearms parts. On Feb. 2, 2016, Kolsuz began his return trip to Istanbul, Republic of Turkey by checking in at Miami International Airport for a flight that took him to Cleveland Hopkins International Airport. He then checked in for a flight that was to take him and his checked luggage through Cleveland Hopkins International Airport and Washington Dulles International Airport before embarking for Istanbul, Republic of Turkey on Turkish Airlines. When Kolsuz arrived at Dulles, his luggage was searched and the firearms parts were discovered. The eighteen handgun barrels, twenty-two 9mm handgun magazines, four .45 caliber handgun magazines, one .357 caliber handgun magazine, and one .22 caliber Glock caliber conversion kit were and are each defense articles listed on the USML, and a license or other written authorization from the DDTC was and is therefore required for the firearms parts to be lawfully exported from the United States. However, Kolsuz and his co-conspirators have never registered with the DDTC, or applied to register with the DDTC, to export defense articles from the United States, and they have never applied for and have never received any licenses or other written authorization from the DDTC to export defense articles from the United States. This case was investigated by the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations.

Theft of Trade Secrets of Inbred Corn Seeds to China – On Oct. 5, 2016, in the Southern District of Iowa, Mo Hailong, a/k/a Robert Mo, a Chinese national, was sentenced to 36 months in prison for conspiracy to steal trade secrets. Mo Hailong was also ordered to serve three years of supervised release following his term of imprisonment. On Dec. 19, 2016, Mo Hailong was ordered to pay restitution in the amount of $425,000. In addition, the Court ordered the forfeiture of two farms in Iowa and Illinois that were purchased and utilized by Mo Hailong and others during the course of the conspiracy. Mo Hailong is a Chinese national who became a lawful permanent resident of the United States. During the course of the conspiracy, Mo Hailong was employed as the Director of International Business of the Beijing Dabeinong Technology Group Company, commonly referred to as DBN. DBN is a Chinese conglomerate with a corn seed subsidiary company, Kings Nower Seed. According to the plea agreement entered on Jan. 27, 2016, Mo Hailong admitted to participating in a long-term conspiracy to steal trade secrets from DuPont Pioneer and Monsanto. Mo Hailong participated in the theft of inbred corn seeds from fields in the Southern District of Iowa and elsewhere for the purpose of transporting the seeds to DBN in China. The stolen inbred, or parent, seeds were the valuable trade secrets of DuPont Pioneer and Monsanto. The investigation was initiated when DuPont Pioneer security staff detected suspicious activity and alerted the FBI. DuPont Pioneer and Monsanto were fully cooperative throughout the investigation. This matter was investigated by the FBI.

Aid to North Korea's Nuclear and Missile Programs – On Sep. 26, 2016, a criminal complaint was unsealed in the District of New Jersey charging four Chinese nationals and a trading company based in Dandong, China, with conspiring to evade U.S. economic sanctions and violating the Weapons of Mass Destruction Proliferators Sanctions Regulations (WMDPSR) through front companies by facilitating prohibited U.S. dollar transactions through the United States on behalf of a sanctioned entity in the Democratic People's Republic of Korea (North Korea) and to launder the proceeds of that criminal conduct through U.S. financial institutions. On Aug. 3, 2016, a U.S. Magistrate Judge in the District of New Jersey signed a criminal complaint charging Ma Xiaohong (Ma) and her company, Dandong Hongxiang Industrial Development Co. Ltd. (DHID), and three of DHID's top executives, general manager Zhou Jianshu (Zhou), deputy general manager Hong Jinhua (Hong) and financial manager Luo Chuanxu (Luo), with conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and to defraud the United States; violating IEEPA; and conspiracy to launder monetary instruments. The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) also imposed sanctions on DHID, Ma, Zhou, Hong and Luo for their ties to the government of North Korea's weapons of mass destruction proliferation efforts. In addition, the department filed a civil forfeiture action for all funds contained in 25 Chinese bank accounts that

allegedly belong to DHID and its front companies. The department has also requested that the federal court in the District of New Jersey issue a restraining order for all of the funds named in the civil forfeiture action, based upon the allegation that the funds represent property involved in money laundering, which makes them forfeitable to the United States. There are no allegations of wrongdoing by the U.S. correspondent banks or foreign banks that maintain these accounts. According to criminal and civil complaints, DHID is primarily owned by Ma and is located near the North Korean border. DHID allegedly openly worked with North Korea-based Korea Kwangson Banking Corporation (KKBC) prior to Aug. 11, 2009, when the OFAC designated KKBC as a Specially Designated National (SDN) for providing U.S. dollar financial services for two other North Korean entities, Tanchon Commercial Bank (Tanchon) and Korea Hyoksin Trading Corporation (Hyoksin). President Bush identified Tanchon as a weapons of mass destruction proliferator in June 2005, and OFAC designated Hyoksin as an SDN under the WMDPSR in July 2009. Tanchon and Hyoksin were so identified and designated because of their ties to Korea Mining Development Trading Company (KOMID), which OFAC has described as North Korea's premier arms dealer and main exporter of goods and equipment related to ballistic missiles and conventional weapons. The United Nations (UN) placed KOMID, Tanchon and Hyoksin on the UN Sanctions List in 2006. In March 2016, KKBC was added to the UN Sanctions List. In Aug. 2009, Ma allegedly conspired with Zhou, Hong and Luo to create or acquire numerous front companies to conduct U.S. dollar transactions designed to evade U.S. sanctions. The complaints allege that from Aug. 2009, to Sep. 2015, DHID used these front companies, established in offshore jurisdictions such as the British Virgin Islands, the Seychelles and Hong Kong, and opened Chinese bank accounts to conduct U.S. dollar financial transactions through the U.S. banking system when completing sales to North Korea. These sales transactions were allegedly financed or guaranteed by KKBC. These front companies facilitated the financial transactions to hide KKBC's presence from correspondent banks in the United States, according to the allegations in the complaints. As a result of the defendants' alleged scheme, KKBC was able to cause financial transactions in U.S. dollars to transit through the U.S. correspondent banks without being detected by the banks and, thus, were not blocked under the WMDPSR program. On July 22, 2019, a federal grand jury in Newark, New Jersey returned an indictment charging Ma, DHID, Zhou, Hong, and Luo with violating IEEPA, conspiracy to violate IEEPA and to defraud the United States, and conspiracy to launder monetary instruments. The case was investigated by the FBI.

Systems and Components for Marine Submersible Vehicles to China – On Sep. 26, 2016, in the Middle District of Florida, Amin Yu was sentenced to 21 months in federal prison for acting in the U.S. as an illegal agent of a foreign government without prior notification to the Attorney General and for conspiring to commit international money laundering. According to the plea agreement dated June 10, 2016, from at least 2002 until Feb. 2014, at the direction of co-conspirators working for Harbin Engineering University (HEU), a state-owned entity in the People's Republic of China, Yu obtained systems and components for marine submersible vehicles from companies in the United States. She then illegally exported those items to the PRC for use by her co-conspirators in the development of marine submersible vehicles – unmanned underwater vehicles, remotely operated vehicles and autonomous underwater vehicles – for HEU and other state-controlled entities. Yu illegally exported items by failing to file electronic export information (EEI), as required by U.S. law, and by filing false EEI. In particular, Yu completed and caused the completion of export-related documents in which she significantly undervalued the items that she had exported and provided false end user information for those items. Previously, on April 21, 2016, an 18-count superseding indictment was unsealed in the Middle District of Florida charging Yu with acting as an illegal agent of a foreign government in the United States without prior notification to the Attorney General, conspiring to defraud the United States and to commit offenses against the United States, committing unlawful export information activities, smuggling goods from the United States, conspiring to and committing international money laundering and making false statements to the U.S. Citizenship and Immigration Services. This case was investigated by the FBI, U.S. Immigration and Customs Enforcement's Homeland Security Investigations, the Internal Revenue Service-Criminal Investigation and the Naval Criminal Investigative Service.

Sensitive Technology to Pakistani Military – On Sep. 1, 2016, in the District of Arizona, Syed Vaqar Ashraf, of Lahore, Pakistan, was sentenced to 33 months in prison. Ashraf previously pleaded guilty to conspiracy to export defense controlled items without a license. Ashraf attempted to procure gyroscopes and illegally ship them to Pakistan so they could be used by the Pakistani military. In an effort to evade detection, Ashraf arranged for the gyroscopes to be purchased in the name of a shell company and caused the gyroscopes to be transshipped to Belgium. Ashraf then traveled to Belgium to inspect the gyroscopes and arrange for their final transport to Pakistan. On Aug. 26, 2014, Ashraf was arrested by the Belgium Federal Police at the request of U.S. Immigration and Customs Enforcement's Homeland Security Investigations (HSI) agents, who had been conducting an undercover investigation of Ashraf's activities. This case was investigated by ICE-HSI and Belgium Federal Police.

Unmanned Aerial Vehicle to China – On Aug. 19, 2016, in the Southern District of Florida, Wenxia Man, a/k/a Wency Man, was sentenced to 50 months in prison for conspiring to export and cause the export of fighter jet engines, an unmanned aerial vehicle – commonly known as a drone – and related technical data to the People's Republic of China in violation of the Arms Export Control Act. Previously, on June 9, 2016, Man was convicted by a federal jury in the Southern District of Florida of one count of conspiring to export and cause the export of defense articles without the required license. According to evidence presented at trial, between approximately March 2011, and June 2013, Man conspired with Xinsheng Zhang, who was located in China, to illegally acquire and export to China defense articles including: Pratt & Whitney F135-PW-100 engines used in the F-35 Joint Strike Fighter; Pratt & Whitney F119-PW-100 turbofan engines used in the F-22 Raptor fighter jet; General Electric F110-GE-132 engines designed for the F-16 fighter jet; the General Atomics MQ-9 Reaper/Predator B Unmanned Aerial Vehicle, capable of firing Hellfire Missiles; and technical data for each of these defense articles. During the course of the investigation, when talking to an undercover HSI agent, Man referred to Zhang as a "technology spy" who worked on behalf of the Chinese military to copy items obtained from other countries and stated that he was particularly interested in stealth technology. This case was investigated by HSI and DCIS.

Defense Articles to Sudan – On Aug. 4, 2016, in the Eastern District of Virginia, Ellias Abdl Halim Ghandi, a/k/a's Eliyas Ghandi, Ellias Woldemariam, and Ellias Ghandi Ahmed, a United States citizen, was sentenced to 40 months' imprisonment, two years' supervised release and $100 special assessment following a plea of guilty on May 18, 2016, to violating the Arms Export Control Act. Ghandi pleaded guilty to a one-count information alleging that he knowingly and willfully attempted to export and exported rifles, pistols, and shotguns, which are defense articles on the U.S. Munitions List, from the United States to Khartoum, Sudan, without first obtaining the required license from the State Department. According to court documents, from May 6, 2012, to Nov. 20, 2014, Ghandi purchased twenty firearms from three firearms dealers on eighteen separate occasions and repeatedly traveled to Khartoum. Ghandi admitted that over the years, he had brought 20-30 guns into Sudan where he said that American guns were popular and sold well. The investigation was conducted by the U.S. Department of Homeland Security, Homeland Security Investigations.

Sensitive Military and Export Controlled Data to China – On July 13, 2016, in the Central District of California, Su Bin, also known as Stephen Su and Stephen Subin, a Chinese national and resident of the People's Republic of China, was sentenced to 46 months' imprisonment, a fine of $10,000 and one year of supervised release. Previously, on March 23, 2016, Su Bin pleaded guilty to participating in a years-long conspiracy to hack into the computer networks of major U.S. defense contractors, steal sensitive military and export-controlled data and send the stolen data to China. A criminal complaint filed in 2014 and subsequent indictments filed in Los Angeles charged Su Bin, a China-based businessman in the aviation and aerospace fields, for his role in the criminal conspiracy to steal military technical data, including data relating to the C-17 strategic transport aircraft and certain fighter jets produced for the U.S. military. Su

was initially arrested in Canada in July 2014, on a warrant issued in relation to this case. Su ultimately waived extradition and consented to be conveyed to the United States in Feb. 2016. In the plea agreement, Su admitted to conspiring with two persons in China from Oct. 2008, to March 2014, to gain unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information and to export that information illegally from the United States to China. As part of the conspiracy, Su would e-mail the co-conspirators with guidance regarding what persons, companies and technologies to target during their computer intrusions. One of Su's co-conspirators would then gain access to information residing on computers of U.S. companies and email Su directory file listings and folders showing the data that the co-conspirator had been able to access. Su then directed his co-conspirator as to which files and folders his co-conspirator should steal. Once the co-conspirator stole the data, including by using techniques to avoid detection when hacking the victim computers, Su translated the contents of certain stolen data from English into Chinese. In addition, Su and his co-conspirators each wrote, revised and emailed reports about the information and technology they had acquired by their hacking activities, including its value, to the final beneficiaries of their hacking activities. Su's plea agreement makes clear that the information he and his co-conspirators intentionally stole included data listed on the U.S. Munitions List contained in the International Traffic in Arms Regulations. Su also admitted that he engaged in the crime for the purpose of financial gain and specifically sought to profit from selling the data the he and his co-conspirators illegally acquired. This case was investigated by the FBI, the U.S. Air Force Office of Special Investigations, and the Justice Department's CRM/OIA and NSD/CES.

Satellite Trade Secrets to Undercover Agent – On July 7, 2016, in the Central District of California, Gregory Allen Justice was arrested by FBI special agents on federal charges of economic espionage and violations of the Arms Export Control Act (AECA) for his attempts to sell sensitive satellite information to a person he believed to be a foreign intelligence agent. Justice worked for a cleared defense contractor as an engineer on military and commercial satellites during his alleged crimes. According to the affidavit in support of the criminal complaint, Justice stole proprietary trade secret materials from his employer and provided them to a person whom he believed to be a representative of a foreign intelligence service, but who was in fact an FBI undercover agent. In addition to their proprietary nature, the documents contained technical data covered by the U.S. Munitions List and therefore controlled for export from the United States under the International Traffic in Arms Regulations, according to the allegations. In exchange for providing these materials, Justice allegedly sought and received cash payments. On May 22, 2017, Gregory Allen Justice pleaded guilty to one count of attempting to commit economic espionage and one count of attempting to violate the AECA; on Sep. 19, 2017, he was sentenced to 60 months in prison. This investigation was conducted by the FBI and the Air Force Office of Special Investigations (AFOSI).

High Tech U.S. Military Hardware to China – On June 29, 2016, in the District of Delaware, Kan Chen of Ningbo, China, in Zhejiang Province, was sentenced to 30 months in prison and three years of supervised release for conspiring to violate the Arms Export Control Act and International Traffic in Arms Regulations; attempting to violate the Arms Export Control Act and International Traffic in Arms Regulations; and violating the International Emergency Economic Powers Act. On June 16, 2015, Chen was arrested by HSI agents on the Northern Mariana Island of Saipan following an eight-month long investigation into his illegal conduct and has remained in custody. He pleaded guilty to the offenses listed above on March 2, 2016. According to court documents, from July 2013, through his arrest in June 2015, Chen caused or attempted to cause the illegal export of over 180 export-controlled items, valued at over $275,000, from the United States to China. Over 40 of those items – purchased for more than $190,000 – were sophisticated night vision and thermal imaging scopes, which are designated by the International Traffic in Arms Regulations as U.S. Munitions List defense articles and can be mounted on automatic and semi-automatic rifles and used for military purposes at night. Given the sensitivity surrounding these military-grade items, Chen devised a scheme to smuggle these items through Delaware and outside the United States. He purchased

the devices via the internet and telephone and had them mailed to several reshipping services in New Castle, Delaware, which provide an American shipping address for customers located in China, accept packages for their customers and then re-shipped them to China. In order to further conceal his illegal activity, Chen arranged for the re-shippers to send the devices to several intermediary individuals, who in turn forwarded the devices to Chen in China. Chen then sent the devices to his customers. During the course of this conduct, Chen made numerous false statements in order to knowingly and willfully evade the export control laws of the United States, including by undervaluing the shipments, unlawfully avoiding the filing of export information with the U.S. government, indicating that he was a natural-born U.S. citizen and providing the address of the reshipping service as his own. During the sentencing hearing, the government noted the lethality of these items when combined with weapons designed for use on a battlefield. For example, the ATN ThOR 640-5x, 640x480-Inch Thermal Weapon Scope, 100 mm, which Chen purchased for $8,428.39, is described by the manufacturer as "an ideal product for force protection, border patrol officers, police SWAT and special operations forces providing them the tools they need to be successful in all field operations both day and night. Uncooled thermal imaging cuts through dust, smoke, fog, haze, and other battlefield obscurants." These rifle scopes, therefore, are weapons of war, and Chen's smuggling and subsequent sale of these military-grade items outside of the United States directly undermines our nation's national security interests. As the government further noted, Chen's conduct was particularly harmful because he sold this military technology indiscriminately. Thus, it could have ended up in any number of nefarious hands – including agents of foreign governments, bad actors and brokers. Once these rifle scopes were exported to China and distributed by Chen to his customers, the military technology contained inside these items could have been reversed engineered or used anywhere in the world for a variety of purposes by oppressive regimes, terrorists, or others to threaten the United States or its allies' military advantage or to commit human rights abuses. This case was investigated by HSI and U.S. Department of Commerce-Bureau of Industry and Security's Office of Export Enforcement.

High-Tech Material Used in Missile Production and Nuclear Applications to Iran – On June 14, 2016, in the Eastern District of New York, Erdal Kuyumcu, the CEO of Global Metallurgy LLC, a company based in Woodside, New York, pleaded guilty to one count of conspiring to violate the International Emergency Economic Powers Act, in connection with the export of specialty metals from the United States to Iran. On Sep. 7, 2017, Kuyumcu was sentenced to 57 months in prison and fined $7,000. As detailed in the criminal information to which he pleaded guilty and other court filings, Kuyumcu, a U.S. citizen, conspired to export from the United States to Iran a metallic powder composed of cobalt and nickel, without having obtained the required license from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC). The metallic powder can be used to coat gas turbine components, including turbine blades, and can be used in aerospace, missile production and nuclear applications. Such specialized metals are closely regulated by the U.S. Department of Commerce to combat nuclear proliferation and protect national security, and exporting them without an OFAC license is illegal. Kuyumcu and others conspired to obtain over 1,000 pounds of the metallic powder from a U.S.-based supplier for export to Iran. To hide the true destination of the goods from the U.S. supplier, Kuyumcu and a co-conspirator arranged for the metallic powder to be shipped first to Turkey and then to Iran. This case was investigated by the Commerce Department and the FBI.

Theft of Valuable Source Code for China – On June 14, 2016, Jiaqiang Xu was charged in the Southern District of New York in a six-count superseding indictment with economic espionage and theft of trade secrets, in connection with Xu's theft of proprietary source code from his former employer, with the intent to benefit the National Health and Family Planning Commission of the People's Republic of China. On May 19, 2017, Xu pleaded guilty to the indictment. On Jan. 17, 2018, Xu was sentenced to five years in prison. Xu was initially arrested by the FBI on Dec. 7, 2015, and subsequently charged on Jan. 6, 2016, by indictment with one count of theft of trade secrets. According to court documents, from Nov. 2010, to May 2014, Xu worked as a developer for a particular U.S. company (the "Victim Company"). As a developer,

Xu enjoyed access to certain proprietary software (the "Proprietary Software"), as well as that software's underlying source code (the "Proprietary Source Code"). The Proprietary Software is a clustered file system developed and marketed by the Victim Company in the U.S. and other countries. A clustered file system facilitates faster computer performance by coordinating work among multiple servers. The Victim Company takes significant precautions to protect the Proprietary Source Code as a trade secret. The Victim Company takes these precautions in part because the Proprietary Software and the Proprietary Source Code are economically valuable, which value depends in part on the Proprietary Source Code's secrecy. In May 2014, Xu voluntarily resigned from the Victim Company. Xu subsequently, in a series of communication with UC agents, uploaded Victim Company's Proprietary Source Code to the UC's computer network. On Dec. 7, 2015, Xu met with UC-2 at a hotel in White Plains, New York (the Hotel). Xu stated, in sum and substance, that Xu had used the Proprietary Source Code to make software to sell to customers, that Xu knew the Proprietary Source Code to be the product of decades of work on the part of the Victim Company, and that Xu had used the Proprietary Source Code to build a copy of the Proprietary Software, which Xu had uploaded and installed on the UC Network (i.e., the Xu Upload). Xu also indicated that Xu knew the copy of the Proprietary Software that Xu had installed on the UC Network contained information identifying the Proprietary Software as the Victim Company's property, which could reveal the fact that the Proprietary Software had been built with the Proprietary Source Code without the Victim Company's authorization. Xu told UC-2 that Xu could take steps to prevent detection of the Proprietary Software's origins – i.e., that it had been built with stolen Proprietary Source Code – including writing computer scripts that would modify the Proprietary Source Code to conceal its origins. Later on Dec. 7, 2015, Xu met with UC-1 and UC-2 at the Hotel. During that meeting, Xu showed UC-2 a copy of what Xu represented to be the Proprietary Source Code on Xu's laptop. Xu noted to UC-2 a portion of the code that indicated it originated with the Victim Company as well as the date on which it had been copyrighted. Xu also stated that Xu had previously modified the Proprietary Source Code's command interface to conceal the fact that the Proprietary Source Code originated with the Victim Company and identified multiple specific customers to whom Xu had previously provided the Proprietary Software using Xu's stolen copy of the Proprietary Source Code. This case was investigated by the FBI.

Tactical Equipment to Insurgent Groups in Syria – On June 10, 2016, in the Eastern District of Virginia, Amin al-Baroudi, a Syrian-born naturalized U.S. citizen, formerly of Irvine, California, was sentenced to 32 months in prison for conspiring to export U.S.-origin goods from the United States to Syria, in violation of sanctions imposed on Syria by the U.S. government. Baroudi pleaded guilty on Jan. 15, 2016, to conspiracy to export U.S. goods to Syria, in violation of the International Emergency Economic Powers Act, 50 U.S.C. §§ 1702 and 1705(a) and (c). According to court documents, Baroudi admitted that from at least Dec. 2011, through March 2013, he and his co-conspirators exported U.S. tactical equipment to Syria for the purpose of supplying and arming Ahrar al-Sham and other insurgent groups in Syria whose stated goal is to overthrow the Assad government and install an Islamic state. Ahrar al-Sham frequently fights alongside Jabhat al-Nusrah, which has been designated by the U.S. State Department as a foreign terrorist organization and operates as al-Qaeda's official branch in Syria. According to court documents, Baroudi and his co-conspirators purchased tens of thousands of dollars-worth of goods from companies and vendors in the United States, consisting largely of tactical equipment such as sniper rifle scopes, night vision rifle scopes, night vision goggles, laser bore sighters, speed loaders and bullet proof vests. Baroudi and his co-conspirators traveled with the goods aboard commercial flights to Turkey and then transported the goods into Syria or provided them to others for transport. Baroudi made two such trips in Feb. and March of 2013. This case was investigated by the FBI, DOC OEE, ICE HSI, California Highway Patrol; the Irvine Police Department; the Orange County, California, Sheriff's Department; and the Regional Computer Forensics Laboratory in Orange County provided significant assistance.

High-Grade Carbon Fiber to China – On June 9, 2016, Fuyi Sun, a/k/a "Frank", a citizen of the People's Republic of China, was charged in a one-count indictment in the Southern District of New York with

attempting to violate the International Emergency Economic Powers Act (IEEPA). On April 21, 2017, Sun pleaded guilty; and on Sep. 6, 2017, he was sentenced to 36 months in prison. On April 13, 2016, Sun was arrested in connection with a scheme to illegally export to China, without a license, high-grade carbon fiber that is used primarily in aerospace and military applications. Sun was arrested after traveling to New York to meet with undercover agents (UCs) in an effort to obtain the specialized fiber, which – due to its military and aerospace applications – requires an export license for export to China. Sun was originally charged April 13, 2016, in a three-count Complaint, with: Count One – attempt to violate the International Emergency Economic Powers Act (IEEPA); Count Two – conspiracy to violate IEEPA; and Count Three – attempt to smuggle goods from the United States. According to Court documents, Sun attempted for years to acquire high-grade carbon fiber for illegal export to China. After traveling to New York from China to finalize the deal, Sun allegedly told the UCs that the carbon fiber he sought was headed to the Chinese military. He then paid tens of thousands of dollars in cash to purchase two cases of it. To avoid law enforcement detection, Sun allegedly directed the UCs to ship the carbon fiber in unmarked boxes and to falsify the shipping documents regarding the contents of the boxes. Courts documents also state that, since approximately 2011, Sun has attempted to acquire extremely high-grade carbon fiber, including Toray type M60JB-3000-50B carbon fiber ("M60 Carbon Fiber"). M60 Carbon Fiber has applications in aerospace technologies, unmanned aerial vehicles (commonly known as "drones") and other government defense applications. Accordingly, M60 Carbon Fiber is strictly controlled – including that it requires a license for export to China – for nuclear non-proliferation and anti-terrorism reasons. In furtherance of his attempts to illegally export M60 Carbon Fiber from the United States to China without a license, Sun contacted what he believed was a distributor of carbon fiber – but which was, in fact, an undercover entity created by HSI and "staffed" by HSI UCs. Sun inquired about purchasing the M60 Carbon Fiber without the required license. In the course of his years-long communications with the UCs and the UC Company, Sun repeatedly suggested various security measures that he believed would protect them from "U.S. intelligence." Among other such measures, at one point, Sun instructed the UCs to use the term "banana" instead of "carbon fiber" in their communications. Consequently, soon thereafter he inquired about purchasing 450 kilograms of "banana" for more than $62,000. In order to avoid detection, Sun also suggested removing the identifying barcodes for the M60 Carbon Fiber, prior to transshipment, and further suggested that they identify the M60 Carbon Fiber as "acrylic fiber" in customs documents. On or about April 11, 2016, Sun traveled from China to New York for the purpose of purchasing M60 Carbon Fiber from the UC Company. During meetings with the UCs, on or about April 11 and 12, 2016, among other things, Sun repeatedly suggested that the Chinese military was the ultimate end-user for the M60 Carbon Fiber he sought to acquire from the UC Company. Sun claimed to have personally worked in the Chinese missile program. Sun also asserted that he maintained a close relationship with the Chinese military, had a sophisticated understanding of the Chinese military's need for carbon fiber, and suggested that he would be supplying the M60 Carbon Fiber to the Chinese military or to institutions closely associated with it. On or about April 12, 2016, Sun agreed to purchase two cases of M60 Carbon Fiber from the UC Company. Sun paid the UCs $23,000 in cash for the carbon fiber. He also paid an additional $2,000 to the UCs as compensation for the risk he believed they were taking to illegally export the carbon fiber to China without a license. This investigation was conducted by DOC, HSI, and DCIS.

High-Tech Electronic Components to Iran – On May 23, 2016, in the Southern District of New York, Ali Reza Parsa, a Canadian-Iranian dual citizen and resident of Canada, was sentenced to three years in prison for his participation in a conspiracy to violate the International Emergency Economic Powers Act (IEEPA) and the Iranian Transactions and Sanctions Regulations (ITSR). Parsa was arrested in Oct. 2014, following an investigation by the FBI and U.S. Department of Commerce's Bureau of Industry and Security (BIS). He pleaded guilty on Jan. 20, 2016. According to court documents, between approximately 2009 and 2015, Parsa conspired to obtain high-tech electronic components from American companies for transshipment to Iran and other countries for clients of Parsa's procurement company in Iran, Tavan Payesh Mad, in violation of U.S. economic sanctions. To accomplish this, Parsa used his Canadian company, Metal PM, to place

orders with U.S. suppliers and typically had the parts shipped to him in Canada or to a freight forwarder located in the United Arab Emirates, and then shipped from these locations to Iran or to the location of his Iranian company's client. Parsa provided the U.S. companies with false destination and end-user information about the components in order to conceal the illegality of these transactions. Parsa's criminal scheme targeted numerous American technology companies. The components that Parsa attempted to procure included cryogenic accelerometers, which are sensitive components that measure acceleration at very low temperatures. Cryogenic accelerators have both commercial and military uses, including in applications related to ballistic missile propellants and in aerospace components such as liquid-fuel rocket engines. In addition, following his arrest and while incarcerated, Parsa continued to violate the IEEPA and the ITSR by conducting business for Metal PM and Tavan Payesh Mad, including by ordering parts from German and Brazilian companies for Iranian customers. Parsa subsequently directed a relative to delete email evidence of his ongoing business transactions while in jail and emphasized the need for secrecy in their dealings. Neither Parsa nor any other individual or entity involved in transactions that gave rise to his conviction applied for or obtained a license from the U.S. Department of the Treasury's Office of Foreign Assets Control for the transactions. This case was investigated by the FBI and Department of Commerce BIS.

Defense Materials to India – On April 14, 2016, in the District of New Jersey, Hannah Robert, the owner of two New Jersey defense contracting businesses, was sentenced to 57 months in prison for conspiring to send sensitive military technical data to India. Previously, on April 1, 2015, Robert pleaded guilty to one count of conspiracy to violate the Arms Export Control Act (22 U.S.C. § 2778). On Oct. 28, 2013, Robert was arraigned for allegedly transmitting military technical drawings to India without first obtaining a license from the U.S. Department of State, in violation of U.S. export laws. She was indicted by a federal grand jury on Oct. 10, 2013, on one count of violating the Arms Export Control Act and one count of conspiracy to violate the act. According to the documents filed in this case and statements made in court, Robert was the founder, owner, and President of One Source USA LLC, a company located at her then-residence in Mount Laurel, N.J., and contracted with the U.S. Department of Defense (DoD) to supply defense hardware items and spare parts pursuant to government contracts. In Sep. 2012, Robert opened a second defense-contracting company, Caldwell Components Inc., based at the same address in Mount Laurel. Along with "R.P," a resident of India, Robert owned and operated a company in India, One Source (One Source India), that manufactured defense hardware items and spare parts in India. From June 2010 to Dec. 2012, Robert and R.P. conspired to export to India defense technical drawings without obtaining the necessary licenses from the U.S. Department of State. The exported technical drawings include parts used in the torpedo systems for nuclear submarines, in military attack helicopters, and in F-15 fighter aircraft. Robert allegedly lied on her bids for DoD contracts, stating that she would be supplying American-made products and that her N.J.-based company was a manufacturer, rather than a dealer, of defense spare parts. One Source USA also subcontracted to other American defense contractors, including those in Sussex County, N.J., and Boca Raton, Fla. Robert provided export-controlled items made in India to these defense contractors in the United States in such a way as to appear to the DoD that the items were manufactured in this country. In addition to United States' sales, Robert and R.P. sold defense hardware items to foreign customers. Robert transmitted export-controlled technical data to R.P. in India so that Robert and R.P. could submit bids to foreign actors, including those in the United Arab Emirates (UAE), to supply them or their foreign customers with defense hardware items and spare parts. Neither Robert nor R.P. obtained approval from the U.S. Department of State for this conduct. On Aug. 23, 2012, R.P. e-mailed Robert from India requesting the technical drawing for a particular military item. R.P.'s e-mail forwarded Robert an e-mail from an individual purporting to be "an official contractor of the UAE Ministry of Defence," and who listed a business address in Abu Dhabi, UAE. The UAE e-mail requested quotations for a bid for the "blanket assembly" for the CH-47F Chinook military helicopter and listed the "End User" for the hardware item as the UAE Armed Forces. Later that same day, Robert replied to R.P.'s e-mail, attaching, among other things, the electronic file for an export-controlled technical drawing titled "Installation and Assy Acoustic

Blankets, STA 120 CH-47F," to be used in the Chinook attack helicopter. Starting in Oct. 2010, Robert transmitted the military drawings for these parts to India by posting the technical data to the password-protected website of a Camden County, N.J., church where she was a volunteer web administrator. This was done without the knowledge of the church staff. Robert e-mailed R.P. the username and password to the church website so that R.P. could download the files from India. Through the course of the scheme, Robert uploaded thousands of technical drawings to the church website for R.P. to download in India. On June 25, 2012, R.P. e-mailed Robert from India, stating in part: "Please send me the church web site username and password." The e-mail was in reference to both an invoice to, and a quote for, an individual known to Robert as a broker of defense hardware items for an end-user in Pakistan. This individual (the "Pakistan trans-shipper") employed a UAE address for shipping purposes. This case was investigated by DoD, DCIS, and DHS HSI Counter Proliferation Investigations.

F-14 Fighter Jet Parts to Iran – On April 5, 2016, in the Northern District of Georgia, Oguzhan Aydin was sentenced to 30 months' imprisonment, 5 years supervised release, $200 special assessment and a $25,000 fine. Aydin pleaded guilty on Oct. 13, 2015, to exporting munitions out of the United States and money laundering. Previously, on Aug. 26, 2014, Aydin was arrested pursuant to an arrest warrant in the Northern District of Georgia. A federal grand jury returned an indictment charging Aydin, Saeid Kamyari, AGM Ltd. Co. and Blue Sky Aviation with violations of the Arms Export Control Act and the International Emergency Economic Powers Act. According to court documents, between Sep. 2009, and Aug. 2010, Kamyari, while in Iran, worked through AGM Ltd. Co., a company located in Tehran, Iran, to procure aircraft parts for the F-14 Fighter Jet and other aircraft parts for shipment from the U.S. to Iran. Aydin, while in the Republic of Turkey, assisted Kamyari through his association with Blue Sky Aviation a/k/a BSA Hava Kargo Ltd. Sti. Using e-mails, Kamyari and Aydin coordinated and arranged through AGM LTD Co. and Blue Sky Aviation, the purchase and export of microcircuits designed for use on F-14 fighter jets and other aircraft parts for shipment from the U.S. through Turkey to Iran. At no time did the co-conspirators obtain a license to export aircraft parts from the U.S. to Iran. This investigation was conducted by DHS.

Sanctions Violations to Aid Iran Government – On March 21, 2016, an indictment was unsealed in the Southern District of New York against Reza Zarrab a/k/a Riza Sarraf, a resident of Turkey and dual citizen of Turkey and Iran; Camelia Jamshidy a/k/a Kamelia Jamshidy, a citizen of Iran; and Hossein Najafzadeh, a citizen of Iran, for engaging in hundreds of millions of dollars-worth of transactions on behalf of the government of Iran and other Iranian entities, which were barred by U.S. sanctions, laundering the proceeds of those illegal transactions and defrauding several financial institutions by concealing the true nature of these transactions. Zarrab was arrested on March 19, 2016, and had his initial court appearance in Miami, Florida, on March 21, 2016. Jamshidy and Najafzadeh remain at large. According to the allegations contained in the indictment, between 2010 and 2015, Zarrab, Jamshidy and Najafzadeh conspired to conduct international financial transactions on behalf of and for the benefit of, among others, Iranian businesses, the Iranian government and entities owned or controlled by the Iranian government. Among the beneficiaries of these schemes were: Bank Mellat, an Iranian government-owned bank designated, during the time of the charged offenses, by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) as a Specially Designated National (SDN) under the Iranian Transactions and Sanctions Regulations, the Iranian Financial Sanctions Regulations and the Weapons of Mass Destruction Proliferators Sanctions Regulations; Mellat Exchange, an Iranian money services business owned and controlled by Bank Mellat; the National Iranian Oil Company (NIOC), identified during the time of the charged offenses by OFAC as an agent or affiliate of Iran's Islamic Revolutionary Guard Corp (IRGC); the Naftiran Intertrade Company Ltd. (NICO), Naftiran Intertrade Company Sarl (NICO Sarl) and Hong Kong Intertrade Company (KHICO), companies located in the United Kingdom, Switzerland and Hong Kong, respectively, that were acting on behalf of NIOC; and the MAPNA Group, an Iranian construction and power plant company. Bank Mellat, NIOC, NICO Sarl, NICO and HKICO are no longer designated as

SDNs and NIOC is no longer identified as an agent or affiliate of the IRGC, though these entities remain "blocked parties," with whom U.S. persons continue to be prohibited generally from engaging in unlicensed transactions or dealings. The scheme was part of an intentional effort to assist the government of Iran in evading the effects of United States and international economic sanctions. Zarrab, Jamshidy, Najafzadeh and their co-conspirators used an international network of companies located in Iran, Turkey and elsewhere to conceal from U.S. banks, OFAC and others that the transactions were on behalf of and for the benefit of Iranian entities. This network of companies includes Royal Holding A.S., a holding company in Turkey; Durak Doviz Exchange, a money services business in Turkey; Al Nafees Exchange, a money services business; Royal Emerald Investments; Asi Kiymetli Madenler Turizm Otom, a company located in Turkey; ECB Kuyumculuk Ic Vedis Sanayi Ticaret Limited Sirketi, a company located in Turkey; and Gunes General Trading LLC; and others. As a result of this scheme, the co-conspirators induced U.S. banks to unknowingly process international financial transactions in violation of the IEEPA. On Oct. 26, 2017, Reza Zarrab pleaded guilty and awaits sentencing. The case was investigated by the FBI.

Technology Equipment to China – On March 2, 2016, Louis Brothers was sentenced in the Eastern District of Kentucky to 93 months in prison for illegally exporting sophisticated technology equipment to the People's Republic of China (PRC) and concealing the unlawful proceeds. The sentence also includes a monetary judgment of $1.1 million. Brothers, a former president and CEO of Valley Forge Composite Technologies, pleaded guilty to the offenses in July 2015. He admitted that from 2009 until 2013, he unlawfully exported microcircuits to the PRC. Under federal law, anyone exporting a defense article, including microcircuits, to the PRC must obtain the permission of the Department of State for the purposes of maintaining national security. According to his plea agreement, Brothers intentionally avoided notifying the Department of State about his activity and labeled his shipments as "computer parts" in order to conceal the true identity of the items. Brothers further admitted that he falsified paperwork to make it appear that the proceeds he received from his business with the PRC were actually profits from a business he owned in Kentucky. The investigation was conducted by the FBI and ICE HSI.

Night Vision Devices to China – On Feb. 29, 2016, Song Il Kim, a/k/a Kim Song Il was sentenced in the District of Utah to 40 months' imprisonment, 36 months supervised release and $100 special assessment after pleading guilty on Dec. 9, 2015, to violating the Arms Export Control Act. Kim attempted to export from the United States to China night vision devices without first obtaining a license from the State Department.

Pressure Transducers to Iran – On Jan. 27, 2016, Sihai Cheng, a citizen of the People's Republic of China (PRC), was sentenced in the District of Massachusetts to nine years imprisonment and $600 special assessment after pleading guilty on Dec. 18, 2015, to two counts of conspiring to commit export violations and smuggle goods from the U.S. to Iran and four counts of illegally exporting U.S. manufactured pressure transducers to Iran. In Feb. 2014, Cheng was arrested by the British authorities on U.S. charges during a trip to the United Kingdom. He was detained in the United Kingdom pending extradition to the United States. Cheng arrived in Boston from the United Kingdom on Dec. 5, 2014. On April 4, 2014, following an international investigation, Cheng and co-defendant Seyed Abolfazl Shahab Jamili, an Iranian national, were indicted along with two Iranian companies, Nicaro Eng. Co. and Eyvaz Technic Manufacturing Co., for conspiring to export American-made pressure transducers to Iran. Pressure transducers can be used in gas centrifuges to enrich uranium and produce weapons-grade uranium. The indictment alleged that between Nov. 2005 and 2012, Cheng supplied thousands of parts that have nuclear applications, including U.S.-origin goods, to Eyvaz, an Iranian company involved in the development and procurement of parts for Iran's nuclear weapons program. In 2011, the Council of the European Union designated Eyvaz as an entity "involved in [Iran's] nuclear or ballistic missile activities" and imposed restrictive measures against it. In so doing, it found that Eyvaz had produced vacuum equipment, which it supplied to two of Iran's uranium nuclear enrichment facilities, Natanz and Fordow, and that it also had supplied pressure transducers to

Kalaye Electric Company, an Iranian company which has been designated by the U.S. and United Nations as a proliferator of Weapons of Mass Destruction. Specifically, the indictment alleged that in 2005, Cheng began doing business with Jamili, who worked for Eyvaz and ran his own importing business in Iran. Beginning in Feb. 2009, Cheng and Jamili conspired with others in the PRC to illegally obtain hundreds of U.S. manufactured pressure transducers manufactured by MKS Instruments, Inc., headquartered in Massachusetts, on behalf of Eyvaz. As a result of the illegal activities of Cheng and his co-conspirators, hundreds of MKS pressure transducers were illegally exported from the U.S. to China. Upon receipt of these parts in China, Cheng caused the MKS pressure transducers to be exported to Eyvaz or Jamili in Tehran, Iran, in violation of U.S. export laws. The indictment further alleged that by 2007, Iran was operating thousands of gas centrifuges at the Natanz uranium enrichment facility. Iran has sought and illicitly obtained MKS pressure transducers to use in its centrifuge plants. Publicly available photographs of Natanz (with then President Mahmoud Ahmadinejad) show numerous MKS pressure transducers attached to Iran's gas centrifuge cascades. Because pressure transducers can be used in gas centrifuges to convert natural uranium into a form that can be used in nuclear weapons, they are subject to export controls and cannot be shipped to China without an export license or to Iran at all. On Jan. 16, 2016, the indictment was dismissed against Jamili. This case was investigated by the FBI, U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) and the Department of Commerce's Office of Export Enforcement.

Military Aircraft Components to UAE, Thailand – On Jan. 15, 2016, John Nakkashian was sentenced in the Central District of California to 2 years' probation, $100 special assessment, and a fine of $1,000 after previously pleading guilty on Aug. 28, 2014, to a 1st Superseding Information. Nakkashian admitted that he knowingly made a false statement on a Shipper's Export Declaration Form that a military gyroscope being shipped to Thailand did not require an export license, when in fact it did. Nakkashian was a Vice President for International Sales at Air Shunt Instruments, Inc. Air Shunt, a Chatsworth, California company that buys and sells aircraft and aerospace components, was charged via criminal information and pleaded guilty in the Central District of California on July 15, 2008. The company was sentenced on July 17, 2008, and ordered to pay a criminal fine of $250,000 and a special assessment of $400 for making false statements on a Shipper's Export Declaration in claiming that a military gyroscope being sent overseas in 2003 did not require an export license, when in fact the item required such a license. Nakkashian was responsible for obtaining the required licenses for such exports. On May 20, 2008, Nakkashian was indicted on four counts of violating the Arms Export Control Act. The indictment alleged that Nakkashian illegally exported components for the J85 engine used on the F-5 fighter jet, and other military items to Dubai, United Arab Emirates, without first obtaining the required export license from the State Department. The indictment also alleged that Nakkashian illegally exported a military gyroscope to Thailand. Nakkashian was arrested on June 16, 2014, after fleeing the country during the investigation. The investigation was conducted by DCIS and ICE.

###