EIB World Trade Headlines

Evolutions In Business • www.eib.com • (978) 256-0438
Fax: (978) 250-4529 • P.O. Box 4008, Chelmsford, MA 01824

Octobedr 15, 2018 – Volume 10, Issue 19

Suburban Chicago Man Guilty of Trying to Illegally Export Guns and Ammunition to Haiti

CHICAGO — A suburban Chicago man has admitted in federal court that he tried to illegally export 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 illegally export 16 handguns, five 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.

*(*Continued On The Following Page)*

NEWSLETTER NOTES

The guilty plea was entered Tuesday in federal court in Chicago. It carries a maximum sentence of ten years in prison. U.S. District Judge Joan Humphrey Lefkow set sentencing for Jan. 29, 2019.

The guilty plea was announced by John R. Lausch, Jr., United States Attorney for the Northern District of Illinois; Celinez Nunez, Special Agent-in-Charge of the Chicago Field Division of the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives; Dan Clutch, Special Agent-in-Charge of the Chicago Field Office of the U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement; and James M. Gibbons, Special Agent-in-Charge of the Chicago office of the 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. The government is represented by Assistant U.S. Attorney William Dunne.

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 backseat. 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.

Commerce Initiates Antidumping Duty (AD) Investigations of Imports of Forged Steel Fittings from Italy, the People's Republic of China (China), and Taiwan and a Countervailing Duty (CVD) Investigation of Imports of Forged Steel Fittings from China

- On October 26, 2017, the Department of Commerce (Commerce) announced the initiation of AD investigations of imports of forged steel fittings from China, Italy, and Taiwan and a CVD investigation of imports of forged steel fittings from China.

*(*Continued On The Following Column)*

The AD and CVD laws provide U.S. businesses and workers with a transparent, quasi-judicial, and internationally accepted mechanism to seek relief from the market-distorting effects caused by injurious dumping and unfair subsidization of imports into the United States, establishing an opportunity to compete on a level playing field.

For the purpose of AD investigations, dumping occurs when a foreign company sells a product in the United States at less than its fair value. For the purpose of CVD investigations, a countervailable subsidy is financial assistance from a foreign government that benefits the production of goods from foreign companies and is limited to specific enterprises or industries, or is contingent either upon export performance or upon the use of domestic goods over imported goods.

The petitioners are Bonney Forge Corporation (Mount Union, PA), and the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union (Pittsburgh, PA).

The products covered by these investigations are carbon and alloy forged steel fittings, whether unfinished (commonly known as blanks or rough forgings) or finished. Such fittings are made in a variety of shapes including, but not limited to, elbows, tees, crosses, laterals, couplings, reducers, caps, plugs, bushings and unions. Forged steel fittings are covered regardless of end finish, whether threaded, socket-weld or other end connections.

While these fittings are generally manufactured to specifications ASME B16.11, MSS SP-79, and MSS SP-83, ASTM A105, ASTM A350 and ASTM A182, the scope is not limited to fittings made to these specifications.

The term forged is an industry term used to describe a class of products included in applicable standards, and does not reference an exclusive manufacturing process. Forged steel fittings are not manufactured from casting. Pursuant to the applicable standards, fittings may also be machined from bar stock or machined from seamless pipe and tube.

All types of fittings are included in the scope regardless of nominal pipe size (which may or may not be expressed in inches of nominal pipe size), pressure rating (usually, but not necessarily expressed in pounds of pressure, e.g., 2,000 or 2M; 3,000 or 3M; 6,000 or 6M; 9,000 or 9M), wall thickness, and whether or not heat treated.

Excluded from this scope are all fittings entirely made of stainless steel. Also excluded are flanges, butt weld fittings, and nipples. Subject carbon and alloy forged steel fittings are normally entered under HTSUS 7307.99.1000, 7307.99.3000, 7307.99.5045, and 7307.99.5060. They also may be entered under HTSUS 7307.92.3010, 7307.92.3030, 7307.92.9000, and 7326.19.0010.

Advisory on the Iranian Regime's Illicit and Malign

FIN-2018-A006
October 11, 2018

Activities and Attempts to Exploit the Financial System
The financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help U.S. financial institutions (particularly banks; money services businesses (MSBs), such as virtual currency administrators and exchangers; and dealers in precious metals, stones, and jewels) better detect potentially illicit transactions related to the Islamic Republic of Iran (Iran). This advisory will also help foreign financial institutions better understand the obligations of their U.S. correspondents, avoid exposure to U.S. sanctions, and address the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) risks that Iranian activity poses to the international financial system.

The Iranian regime has long used front and shell companies to exploit financial systems around the world to generate revenues and transfer funds in support of malign conduct, which includes support to terrorist groups, ballistic missile development, human rights abuses, support to the Syrian regime, and other destabilizing actions targeted by U.S. sanctions. These advisory highlights the Iranian regime's exploitation of financial institutions worldwide, and describes a number of typologies used by the regime to illicitly access the international financial system and obscure and further its malign activity. It also provides red flags that may assist financial institutions in identifying these methods.2 Additionally, this advisory is intended to assist financial institutions in light of the United States' withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the re-imposition of U.S. sanctions previously lifted under the JCPOA following the 90- and 180-day wind-down periods for certain activities, while also reminding financial institutions of regulatory obligations under the Bank Secrecy Act (BSA) and the Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA).

Iran's Abuse of the International Financial System

Some of the methods used by the Iranian regime to access the financial system through covert means and to further its malign activities include misusing banks and exchange houses, operating procurement networks that utilize front or shell companies, exploiting commercial shipping, and masking illicit transactions using senior officials, including those at the Central Bank of Iran (CBI).

*(*Continued On The Following Column)*

Iran also has a history of using precious metals to evade sanctions and gain access to the financial system and may seek to use virtual currencies in the future. Often, these e orts serve to fund the regime's nefarious activities, including providing funds to the Islamic Revolutionary Guard Corps (IRGC) and its Islamic Revolutionary Guard Corps-Qods Force (IRGC-QF), as well to Lebanese Hizballah, Hamas, and other terrorist groups.

The Iranian Regime's Use of CBI Officials and Exchange Houses to Facilitate Malign Activity

Use of CBI Officials

Senior officials of the CBI have played a critical role in enabling illicit networks, using their official capacity to procure hard currency and conduct transactions for the bene t of the IRGC-QF and its terrorist proxy group, Lebanese Hizballah.4 The CBI has also been complicit in these activities.

On May 15, 2018, the Office of Foreign Assets Control (OFAC) designated then-CBI Governor Valiollah Seif and the assistant director of the CBI's International Department, Ali Tarzali, adding them to OFAC's List of Specially Designated Nationals and Blocked Persons (SDN List) for conducting transactions through Iraq's banking sector for the bene t of the IRGC-QF and Lebanese Hizballah, which has acted as a proxy for the IRGC-QF. Specifically, Valiollah Seif conspired with the IRGC-QF to move millions of dollars, in a variety of currencies, through the international financial system to allow the IRGC-QF to fund its activities abroad. Seif also supported the transfer of IRGC-QF-associated funds to al-Bilad Islamic Bank, an Iraq-based bank that was also designated by OFAC. Ali Tarzali worked with Lebanese Hizballah and proposed that the terrorist group send funds through al-Bilad Islamic Bank. On May 15, 2018, OFAC also designated the Chairman and Chief Executive of al-Bilad Islamic Bank, who acted as an intermediary to enable and conceal these transactions. Financial institutions should be aware that the U.S. Department of the Treasury has repeatedly observed CBI officials and the IRGC-QF using regional financial institutions as intermediaries to conceal illicit transactions. In exercising appropriate due diligence, financial institutions should be aware that some counterparty financial institutions may not be equipped to identify or address CBI officials' deceptive transactions.7 IRGC-QF front companies are known to retrieve funds—some of which are generated by the sale of Iranian oil—in various currencies from foreign bank accounts held by the CBI and then transfer the funds back to Iran.

*(*Continued On The Following Page)*

Use of Exchange Houses

financial institutions are also advised to exercise appropriate due diligence when dealing with transactions involving exchange houses that may have exposure to Iran or Iranian persons, given that the Iranian regime, senior CBI officials, and the CBI have used such entities to conceal the origin of funds and procure foreign currency for the IRGC-QF.

For example, on May 10, 2018, the United States, in a joint action with the United Arab Emirates (UAE), disrupted an extensive currency exchange network in Iran and the UAE. The network procured and then transferred millions of U.S. dollar-denominated bulk cash through the UAE to the IRGC-QF. As part of this joint action, OFAC designated six individuals and three entities, including Jahan Aras Kish, the Joint Partnership of Mohammadreza Khedmati and Associates, and the Rashed Exchange. The CBI was complicit in the IRGC-QF's scheme, actively supported this network's currency conversion, and enabled it to access funds that it held in its foreign bank accounts. To mask ties to Iran and particularly to the IRGC-QF, this network of cash couriers and currency exchangers established the three now-designated front companies. At least one of these companies, the Rashed Exchange, advertised its currency exchange and international money transfer business all over the world on its website and through social media in an effort to portray its activities as legitimate, while in reality its management was using the company to facilitate the transfers for the IRGC-QF. Khedmati, the managing director of Rashed Exchange, also worked with the IRGC-QF to forge documents to conceal their illicit financial activities from UAE authorities. Using these front companies, these individuals and entities procured and transferred millions in U.S. dollar-denominated bulk cash to the IRGC-QF to fund its malign activities and regional proxy groups.

As financial institutions are aware, during previous periods of heightened sanctions pressure, Iran relied heavily on third-country exchange houses and trading companies to move funds to evade sanctions. As the sanctions on Iran that were lifted under the JCPOA are coming back into effect, Iranian financial institutions can be expected to increase the use of these or other evasive practices. These practices include the use of third-country exchange houses or trading companies to act as money transmitters in processing funds transfers through the United States to third-country beneficiaries, in support of business with Iran that is not exempt or otherwise authorized by OFAC. These third-country exchange houses or trading companies frequently lack their own U.S. dollar accounts and instead rely on the correspondent accounts of their regional banks to access the U.S. financial system. Often these entities are located in jurisdictions considered high risk for transactions.

*(*Continued On The Following Column)*

OFAC's January 10, 2013 advisory identified the following evasive practices used by such third- country exchange houses or trading companies: omission of references to Iranian addresses, omission of names of Iranian persons or entities in the originator or beneficiary fields, and transmission of funds without referencing the involvement of Iran or the designated persons.

Financial institutions should be aware when monitoring payments involving third-country exchange houses or trading companies that a financial institution may be processing commercial transactions related to Iran or Iranian persons. As appropriate, financial institutions should consider (1) requesting additional information from correspondents on the nature of such transactions and the parties involved; (2) while monitoring these payments, conducting account and transaction reviews for individual exchange houses or trading companies that have repeatedly violated or attempted to violate U.S. sanctions against Iran; and (3) contacting their correspondents that maintain accounts for, or facilitate transactions on behalf of, third-country exchange houses or trading companies that engage in one of the above-referenced examples in order to request additional information and to alert them to the use of these practices.

Iran's Use of Procurement Networks

Malign Iran-related actors use front and shell companies12 around the world to procure technology and services that allow them to evade sanctions and continue their destabilizing behaviors. Through these procurement networks, Iran has gained goods and services related to currency counterfeiting, dual-use equipment, and the commercial aviation industry. As part of a risk-based approach, financial institutions should familiarize themselves with these deceptive practices and take steps to avoid direct or indirect facilitation of them.

Printing Equipment and Materials for Counterfeiting Currency

In November 2017, OFAC designated two individuals, Reza Heidari and Mahmoud Seif, and four entities, Pardazesh Tasvir Rayan Co., ForEnt Technik GmbH Co., Printing Trade Center GmbH, and Tejarat Almas Mobin Holding, for their respective roles assisting the IRGC-QF to counterfeit currency. This network used two German-based front companies to deceive European suppliers, circumvent European export restrictions, and surreptitiously procure advanced printing machinery, security printing machinery, and raw materials such as watermarked paper and specialty inks. The network used these items to print counterfeit Yemeni bank notes for the IRGC- QF. Mahmoud Seif was previously involved with the procurement of weapons for the IRGC-QF.

Dual-Use Equipment Procurement for Ballistic Missile Proliferation

*(*Continued On The Following Page)*

In February 2017, OFAC designated multiple individuals and entities that are part of the Abdollah Asgharzadeh network for the procurement of dual-use and other goods on behalf of organizations involved in Iran's ballistic missile programs. This network coordinated procurement through intermediary companies that obfuscated the final recipient of the goods. Asgharzadeh and his associates relied on a network of trusted China-based brokers and their companies to assist his procurement of dual-use and other goods.

Commercial Aviation Industry

Designated Iranian airlines and their agents and affiliates have used deceptive schemes to procure aviation-related materials using front companies. Treasury has issued numerous rounds of sanctions related to e orts by designated Iranian airlines to evade sanctions via the use of front or shell companies financial institutions providing services to the commercial aviation industry should be aware of prior actions by designated Iranian airlines to evade sanctions, and they are advised to exercise appropriate due diligence to ensure compliance with legal requirements. Foreign financial institutions are reminded that they may be subject to sanctions for knowingly conducting significant transactions for or with certain Iran-related persons16 (such as Mahan Air, Caspian Air, Dena Airways, Meraj Air, Pouya Air, Al-Naser Wings Airlines, Syrian Air, Khors Aircompany, Dart Airlines, and UM Air), including prohibitions or strict conditions on their ability to open or maintain correspondent or payable-through accounts in the United States. Non-U.S. persons, including foreign financial institutions, may also be subject to designation and listing on the SDN List for, e.g., providing material support to designated Iranian airlines.

Mahan Air

For many years, the Iranian commercial airline Mahan Air has transferred weapons, funds, and people on behalf of the IRGC-QF and provided support to the Syrian Assad regime and Lebanese Hizballah. In 2011, OFAC designated Mahan Air for providing financial, material, and technological support to the IRGC-QF. To evade sanctions, Mahan Air front companies have negotiated sales contracts and obtained U.S. parts and services for Mahan Air's aircraft in violation of U.S. sanctions.17 These front companies facilitate the transfer of funds to vendors and service providers on behalf of Mahan Air, while also aiding in the procurement of goods, such as aviation parts and services from neighboring countries, Europe, and Asia. The aviation- related materials are then shipped to either the same company, or a different front company, sometimes in another country, to be forwarded to Iran. Mahan Air has moved payments through several front companies and financial institutions in the United States, Canada, the United Kingdom, Belize, France, Belgium, Czech Republic, the UAE, Bahrain, Saudi Arabia, Kyrgyzstan, Sri Lanka, and Bangladesh.

*(*Continued On The Following Column)*

Mahan Air and other designated Iranian airlines' use of front companies is illustrated by recent Treasury actions targeting a procurement network. For example, on May 24, 2018, Treasury designated a network of Turkish front companies that procured U.S.-origin parts for Mahan Air. This network purchased aviation parts—including export-controlled U.S. goods such as U.S.- origin engines—from foreign vendors. The parts were delivered to Istanbul and then forwarded to Mahan Air. OFAC has previously designated airlines in Ukraine, Kyrgyzstan, and Iraq that have served as intermediaries for Mahan Air to acquire aircraft, as well as front companies in the UAE, Thailand, Turkey, and the United Kingdom that purchase parts or facilitate payments on behalf of Mahan Air. For example, in May 2015, Treasury designated Iraq-based Al-Naser Airlines, now operating as Al-Naser Wings Airlines, for purchasing nine Airbus aircraft for Mahan Air from unwilling European suppliers. Al-Naser Airlines also attempted to purchase at least two Airbus aircraft located in the United States for Mahan Air, with payments for the planes wired from the account of a Dubai-based general trading company. Additionally, on July 9, 2018, Treasury designated a Malaysia-based general sales agent (GSA) of Mahan Air, Mahan Travel and Tourism Sdn Bhd, which provides Mahan with reservation and ticketing services. This action notified to the aviation community of the sanctions risk of maintaining commercial relationships with Mahan Air.19 Likewise, on September 14, 2018, Treasury designated Thailand-based My Aviation Company Limited for acting for or on behalf of Mahan Air. This Thailand-based company disregarded numerous U.S. warnings, issued publicly and delivered bilaterally to the Thai government, to sever ties with Mahan Air.

Iran-Related Shipping Companies' Access to the financial System

During previous periods of heightened sanctions pressure, Treasury identified Iranian or Iran-related companies using deceptive shipping practices to evade U.S. sanctions. As detailed in previous OFAC advisories and designation actions, these practices include: the use of falsified documents,22 and the involvement of third parties, such as brokers and trading companies, to mask the underlying payments and business activity with Iran.23 For example, in the pre-JCPOA period, Treasury identified shipping companies around the world that falsified documents to hide ships docking in Iranian ports and the accompanying trade-related payments. In addition, in the past, as the United States has added entities or individuals to OFAC's SDN List, there have been instances where a vessel's ownership or operation was transferred from a newly-designated person to a front company or other person acting for or on behalf of the designated person.

*(*Continued On The Following Page)*

As the sanctions on Iran that were lifted under the JCPOA come back into effect following the 90-and 180-day wind-down periods, Iranian shipping companies may return to the use of these or other evasive practices. financial institutions may see indications of these deceptive shipping practices in the information contained in international wires, payment requests, and letters of credit. Documents may also be falsified, and include bills of lading and shipping invoices to conceal shipping routes, embarkation ports, or shipping agents. Financial institutions may and maritime databases and reports—such as those generated by the International Maritime Bureau or other available services—helpful when verifying trade-related documents. financial institutions should be aware of changes regarding the issuing or writing of letters of credit and other trade- related financial transactions. Financial institutions should report those changes in their SAR financial lings if the changes appear to be related to malign activity. In addition, among other deceptive conduct, Iranian vessels may attempt to hide their origin and purpose by potentially fabricating vessel registration and ag credentials at ports of call and canal entrances. Malign Iran-related actors and sanctioned entities engage in these activities to bypass financial institutions' SDN letters so they may evade sanctions. financial institutions should continue to conduct appropriate due diligence to ensure they are not directly or indirectly providing services to sanctioned parties.

The Iranian Regime's Illicit Use of Precious Metals

Iran has previously used precious metals, such as gold, to evade U.S. sanctions and facilitate the sale of Iranian oil and other goods abroad. In response to these schemes, the United States enacted sanctions specifically targeting Iran's trade in precious metals, including section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012. As the United States re-imposes sanctions lifted under the JCPOA, financial institutions should be aware of prior schemes used by entities with a nexus to Iran to evade sanctions using gold and other commodities.

Virtual Currency

Since 2013, Iran's use of virtual currency includes at least $3.8 million worth of bitcoin-denominated transactions per year. While the use of virtual currency in Iran is comparatively small, virtual currency is an emerging payment system that may provide potential avenues for individuals and entities to evade sanctions. Despite public reports that the CBI has banned domestic financial institutions from handling decentralized virtual currencies, individuals and businesses in Iran can still access virtual currency platforms through the Internet. For example, virtual currency can be accessed through: (1) Iran-located, Internet-based virtual currency exchanges; (2) U.S.- or other third country-based virtual currency exchanges; and (3) peer-to-peer (P2P) exchangers.

*(*Continued On The Following Column)*

Institutions should consider reviewing block chain ledgers for activity that may originate or terminate in Iran. Institutions should also be aware that the international virtual currency industry is highly dynamic; new virtual currency businesses may incorporate or operate in Iran with li le notice or footprint. Further, P2P exchangers—natural or legal persons who offer to buy, sell, or exchange virtual currency through online sites and in-person meetups—may offer services in Iran. These P2P exchangers may operate as unregistered foreign MSBs in jurisdictions that prohibit such businesses; where virtual currency is hard to access, such as Iran; or for the purpose of evading the prohibitions or restrictions in place against such businesses or virtual currency exchanges and other similar business in some jurisdictions. Institutions can utilize technology created to monitor open block chains and investigate transactions to or from P2P exchange platforms.

Activity of these exchangers may involve wire transactions from many disparate accounts or locations combined with transfers to or from virtual currency exchanges. These transactions may occur when account holders fund an account or withdraw value from an account, especially if the foreign exchanger operates in multiple currencies. financial institutions and virtual currency providers that have BSA and U.S. sanctions obligations should be aware of and have the appropriate systems to comply with all relevant sanctions requirements and AML/CFT obligations. Sanctions requirements may include not only screening against the SDN List but also appropriate steps to comply with other OFAC-administered sanctions programs, including those that impose import and/or export restrictions with respect to particular jurisdictions.26 Further, a non-U.S.-based exchanger or virtual currency provider doing substantial business in the United States is subject to AML/CFT obligations and OFAC jurisdiction.

U.S. individuals and institutions involved in virtual currency should be aware of OFAC's March 2018 Frequently Asked Questions (FAQs) on sanctions issues associated with virtual currencies. The FAQs remind U.S. persons that their compliance obligations with respect to transactions are the same, regardless of whether a transaction is denominated in virtual currency or not. OFAC also states as a general matter that U.S. persons and persons otherwise subject to OFAC jurisdiction, including rms subject to OFAC jurisdiction that facilitate or engage in online commerce or process transactions using "digital currency," are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions. Prohibited transactions include transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate prohibitions imposed by OFAC under various sanctions authorities. Additionally, persons that provide financial, material, or technological support for or to a designated person may be designated by OFAC under the relevant sanctions authority.

*(*Continued On The Following Page)*

Financial Action Task Force's Findings Related to Iran's Anti-Money Laundering/Combating the Financing of Terrorism Regime

The financial Action Task Force (FATF) has listed Iran as a jurisdiction with systemic deficiencies in its AML/CFT regime. Despite Iran's commitment in June 2016 to an action plan with the FATF to address its AML/CFT deficiencies, Iran has failed to complete the majority of its action plan. The FATF therefore continues to call upon its members and all jurisdictions to advise their financial institutions to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons from Iran.

In addition to keeping Iran on its Public Statement, on June 29, 2018, the FATF expressed disappointment with Iran's failure to implement its action plan, and it reiterated its concern with the terrorist nuancing risk emanating from Iran and the threat this poses to the international financial system. The FATF noted that Iran "should fully address its remaining action items, including by: (1) adequately criminalizing terrorist nuancing, including by removing the exemption for designated groups 'attempting to end foreign occupation, colonialism and racism'; (2) identifying and freezing terrorist assets in line with the relevant United Nations Security Council resolutions; (3) ensuring an adequate and enforceable customer due diligence regime; (4) ensuring the full independence of the financial Intelligence Unit and requiring the submission of STRs [Suspicious Transaction Reports] for attempted transactions; (5) demonstrating how authorities are identifying and sanctioning unlicensed money/value transfer service providers; (6) ratifying and implementing the Palermo and TF [Terrorist Financing] Conventions and clarifying the capability to provide mutual legal assistance; (7) ensuring that financial institutions verify that wire transfers contain complete originator and beneficiary information; (8) establishing a broader range of penalties for violations of the ML [Money Laundering] offense; and (9) ensuring adequate legislation and procedures to provide for confiscation of property of corresponding. The FATF will decide upon the appropriate action in October 2018 if Iran has not by then enacted the necessary amendments to its AML and CFT laws and ratified the Terrorist Financing and Palermo Conventions. All available advisories on FATF Plenaries, including previous years, are available at https://www. ncen.gov/resources/advisories bulletins fact-sheets/advisories.

Red Flags Related to Deceptive Iranian Activity

The following red flags may help financial institutions identify suspicious activity involving the schemes discussed above. In applying these red flags, financial institutions are advised that no single transactional red ag necessarily indicates suspicious activity, and institutions should ensure that their assessments are in line with their internal risk profile.

*(*Continued On The Following Column)*

Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer's historical financial activity and the existence of other red flags, before determining that a transaction is suspicious. financial institutions should also perform additional inquiries and investigations where appropriate. Foreign financial institutions may and the information beneficial for their risk and threat assessments and suspicious transaction reporting requirements. The appropriate financial crimes compliance/sanctions compliance within the financial institution should be apprised of any transactions that are determined to involve Iran.

Illicit Activity by the CBI or Its Officials

Use of Personal Account. The CBI or CBI officials route transactions to personal accounts instead of central bank or government-owned accounts. Individuals or entities with no central bank or government affiliation withdraw funds from such accounts.

Unusual Wire Transfers. The CBI engages in multiple wire transfers to banks or financial institutions that the CBI would not normally engage in, or that are not related to traditional central bank activity.

Use of Forged Documents. Front companies acting for or on behalf of designated persons use forged documents to conceal the identity of parties involved in the transactions. For example, as a part of the IRGC-QF's currency exchange network scheme, documents were forged by an IRGC-QF front company manager to mislead authorities and conceal the true customers of the entities involved in the scheme.

Illicit Activity through Exchange Houses

Use of Multiple Exchange Houses. Customers may have transactions moving through multiple exchange houses, adding additional fees and costs as they progress through the system. The fees, number of transactions, and pa erns of transactions are atypical to standard and customary commercial practices. Multiple Depositors. Account holders that receive deposits—that do not appear to match the customer's profile or provided documentation—from numerous individuals and entities.

Use of Procurement Networks

Shell or Front Companies. Transactions involving companies that originate with, or are directed to, entities that are shell corporations, general "trading companies", or companies that have a nexus with Iran. For example, a company has an affiliate in Iran or is owned by individuals known to be loyal to the Iranian regime, and appears to lack a general business purpose. Iran uses front companies incorporated across the world, including in Asia and Europe.

*(*Continued On The Following Page)*

Other indicators of possible shell companies include opaque ownership structures, individuals/entities with obscure names that direct the company, or business addresses that are residential or co- located with other companies. Suspicious Declarations. Declarations of information that are inconsistent with other information, such as previous transaction history or nature of business. Declarations of goods that are inconsistent with the associated transactional information. Unrelated Business. Transactions that are directed to companies that operate in unrelated businesses, and which do not seem to comport with the Customer Due Diligence (CDD) and other customer identification information collected during client onboarding and subsequent refreshes.

Illicit Procurement of Aircraft Parts

Use of Front Companies and Transshipment Hubs to Source Aircraft Parts. financial institutions that facilitate commercial aviation-related financial transactions where the beneficial ownership of the counterparty is unknown and the delivery destination is a common transshipment point for onward delivery to Iran. Iran-linked persons have attempted to source U.S.-origin aircraft and related parts from third countries known to be hubs for maintenance, repair, and overhaul operations, and then use front companies located in third-countries to conceal or obfuscate the ultimate Iranian beneficiary of the U.S.-origin aircraft, parts, and aviation-related materials.

Misrepresentation of Sanctions. Misrepresenting to suppliers, dealers, brokers, re-insurers, and other intermediaries that sanctions against Iran have been lifted or are no longer applicable as a result of the JCPOA, or falsely claiming without supporting documentation that an OFAC license has been obtained.

Iran-Related Shipping Companies' Access to the U.S. financial System

Incomplete and Falsified Documentation. Transactions and wire transfers that include bills of lading with no consignees or involving vessels that have been previously linked to suspicious financial activities. Documentation, such as bills of lading and shipping invoices, submitted with wire and payment requests that may appear to be falsified, or with key information omitted, in an attempt to hide the Iranian nexus.

Inconsistent Documentation for Vessels Using Key Ports. Inconsistencies between shipping- related documents and maritime database entries that are used for conducting due diligence. For example, the maritime database may indicate that a vessel docked in an Iranian port, even though this information is not included in the shipping documents submitted to financial institutions for payment processing.

*(*Continued On The Following Column)*

Major ports in Iran are Bandar Abbas, Assaluyeh, and Bandar-e Emam Khomenyi, which is also known as Abadan. Port cities on the Gulf include: Ahvaz, Bushehr, Bandar-e Lengeh, Bandar-e Mahshahr, Chabahar, Kharg Island, and Lavan Island. Kharg Island and Lavan Island are major oil and gas ports.

Previous Ship Registration to Sanctioned Entities. Vessels whose ownership or operation is transferred to another person—following OFAC's designation of its owner or operator—on behalf of the designated person, but the designated owner or operator maintains an interest in the vessel.

Suspicious Funds Transfers

Lack of Information Regarding Origin of Funds. Wire transfers or deposits that do not contain any information about the source of funds, contain incomplete information about the source of funds, or do not match the customer's line of business. Unusual or Unexplainable Wire Transfers. Multiple, unexplained wire transfers and transfers that have no apparent connection to a customer's pro le. For example, individuals may claim that the unusually high-value wire transfers they receive from one or more foreign countries are merely funds sent from relatives in Iran. In addition, wire transfers to accounts in the United States from high-risk jurisdictions that have no apparent connection to the customer's line of business. Using Funnel Accounts. Third parties from across the United States who deposit funds into the accounts of U.S.-based individuals with ties to Iran. The deposits and associated transactions do not match the account holder's normal geographical footprint, and the source of the funds is unknown or unclear.

Structuring Transactions. U.S. persons send or receive money to or from Iran by structuring the cash portion of the transactions to avoid the currency transaction reporting threshold of $10,000. Individuals returning to the United States from Iran also may make large deposits of monetary instruments rather than cash.

Gold. Given Iran's prior use of gold as a substitute for cash to evade U.S. sanctions, financial institutions should consider conducting additional due diligence on transactions related to precious metals, particularly in geographic regions in close proximity to Iran (such as Turkey) that engage in signi can't gold-related transactions. Additionally, financial institutions may notice transactions not obviously linked to Iran, but related to the purchase of unusually high volumes of gold.

*(*Continued On The Following Page)*

Virtual Currency

Logins from Iranian Internet Protocol Addresses or with Iranian Email. Internet Protocol (IP) login activity from entities in Iran or using an Iranian email service in order to transact virtual currencies through a virtual currency exchange. In such cases, financial institutions may also be able to provide associated technical details such as IP addresses with time stamps, device identifiers, and indicators of compromise that can provide helpful information to authorities. Payments to/from Iranian Virtual Currency Entity. A customer or correspondent payment to or from virtual currency exchanges that appear to be operating in Iran.

Peer-to-Peer (P2P) Exchangers. Unexplained transfers into a customer account from multiple individual customers combined with transfers to or from virtual currency exchanges. Wire transfers are usually associated with funding an account or withdrawing value, especially with foreign exchanges that may operate in multiple currencies. FinCEN expects that Iranian financial institutions, the Iranian regime, and its o cials will increase their e orts to evade U.S. sanctions to fund malign activities and secure hard currency for the Government of Iran, following the re-imposition of sanctions lifted under the JCPOA. Treasury and the U.S. Government are interested in information related to Iran's e orts outlined in this advisory, as well as information pertaining to how Iran or Iranian entities subject to sanctions, including the CBI, otherwise evade the sanctions and access the U.S. financial system.

U.S. Sanctions

U.S. primary sanctions on Iran are those sanctions administered by OFAC that broadly prohibit U.S. persons and U.S.-owned or -controlled foreign entities from engaging in virtually all transactions or dealings with or involving Iran, the Government of Iran, or Iranian financial institutions, unless the transactions are exempt from regulation or expressly authorized by the U.S. Government.39 These prohibitions also apply to transactions in or transiting through the United States, as well as other types of activities. Section 560.204 of the Iranian Transactions and Sanctions Regulations (ITSR) prohibits the exportation of goods, services (including financial services), or technology directly or indirectly from the United States, or by a U.S. person, to Iran. Pursuant to this provision, U.S. financial institutions are prohibited from opening or maintaining correspondent accounts for or on behalf of Iranian financial institutions. Absent an exemption or OFAC authorization, foreign persons, including foreign financial institutions, are prohibited from processing transactions to or through the United States in violation of this provision, including transactions through U.S. correspondent accounts for or on behalf of Iranian financial institutions, other Iranian persons, or where the benefit is otherwise received in Iran.

*(*Continued On The Following Column)*

The importation into the United States of any goods or services of Iranian origin or owned or controlled by the Government of Iran is also prohibited unless exempt from regulation or expressly authorized by the U.S. Government. There are also prohibitions on re-exports by non- U.S. persons of goods with 10 percent or more controlled U.S. origin content.

U.S. persons are also subject to broad prohibitions on dealings with, and must block the property and interests in property of, among others, Iran-related persons designated pursuant to authorities targeting specific malign conduct, such as support for terrorism, proliferation of weapons of mass destruction or their means of delivery, and human rights abuses. All Iranian financial institutions are blocked under Executive Order 13599 and section 560.211 of the ITSR and, absent an exemption or OFAC authorization, U.S. persons must block the property and interests in property of all Iranian financial institutions.

Pursuant to the Iranian financial Sanctions Regulations (IFSR) and multiple statutory and executive authorities, foreign financial institutions may be subject to sanctions for knowingly conducting significant transactions for or with certain Iran-related persons, including prohibitions or strict conditions on their ability to open or maintain correspondent or payable-through accounts in the United States. Non-U.S. persons, including foreign financial institutions, may also be subject to blocking sanctions for, e.g., providing material support to designated persons. U.S. and non-U.S. financial institutions should be conscious of their obligations under OFAC sanctions to prevent any use (both direct and indirect) of their U.S. correspondent accounts for transactions involving an Iranian financial institution. OFAC has issued penalties to both U.S. and non-U.S. financial institutions for processing prohibited transactions through the U.S. financial system that involve an indirect, underlying interest of Iranian individuals and entities, including Iranian financial institutions. As a result, the industry should continue to develop controls designed to curtail indirect involvement of Iranian persons in transactions that transit through or otherwise involve the U.S. financial system. In many cases, this requires institutions to employ higher Know-Your- Customer (KYC) and CDD requirements for Iranian entities or clients who do business with Iran. In addition, U.S. and non-U.S. financial institutions should continue to implement robust and multi-tiered levels of screening and review for transactions originating from or otherwise involving jurisdictions in close proximity to Iran. financial institutions engaged in cross-border wire activity should be aware of transactions involving jurisdictions with strong geographical and economic ties to Iran. These practices generally result in significant oversight of correspondent accounts that may involve Iranian interests, as well as create a relatively high-degree of vigilance related to payments and funds transfers on behalf of Iran-related individuals and entities.

(*Continued On The Following Page)

Reminder of Regulatory Obligations for U.S. financial Institutions

Consistent with existing regulatory obligations, U.S. financial institutions should take reasonable, risk-based steps to identify and limit any exposure they may have to funds and other assets associated with individuals and entities involved in laundering illicit proceeds, including those associated with sanctions evasion. Reminder of AML and Regulatory Obligations for U.S. financial Institutions Regarding Due Diligence, Correspondent Accounts, CISADA, and Suspicious Activity Reporting FinCEN is providing the information in this advisory to assist U.S. financial institutions in meeting these risk-based due diligence obligations and to help identify individuals who are providing financial facilitation for or on behalf of sanctioned individuals and entities.

Enhanced Due Diligence Obligations for Private Banking Accounts

In addition to these general risk-based due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, U.S. financial institutions have regulatory obligations to implement a due diligence program for private banking accounts held for non-U.S. persons that is designed to detect and report any known or suspected money laundering or other suspicious activity.

Customer Due Diligence and Identification of Beneficial Owners of New Legal Entity Accounts

As of May 11, 2018, FinCEN's CDD Rule requires banks; brokers or dealers in securities;
mutual funds; and futures commission merchants and introducing brokers in commodities to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions. This could facilitate the identification of legal entities that may be owned or controlled by individuals and entities impacted by Iran-related sanctions.

General Obligations for Correspondent Account Due Diligence and Anti-Money Laundering Programs

*(*Continued On The Following Column)*

U.S. financial institutions also are reminded to comply with their general due diligence obligations under 31 CFR § 1010.610(a), in addition to their general AML Program obligations under 31 U.S.C. § 5318(h) and its implementing regulations. As required under 31 CFR § 1010.610(a), covered financial institutions should ensure that their due diligence programs, which address correspondent accounts maintained for foreign financial institutions, include appropriate, specific, risk-based, and, where necessary, enhanced policies, procedures, and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered, or managed in the United States.

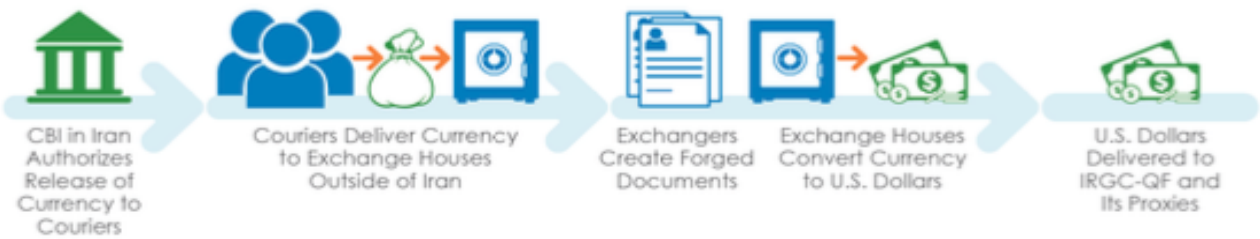
Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010

FinCEN also reminds U.S. banks of the reporting requirements associated with Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) under 31 CFR § 1060.300, upon receipt of a written request from FinCEN, to inquire of a specified foreign bank for which it maintains a correspondent account, for information with respect to the following: whether the foreign bank maintains a correspondent account for, or has processed transfers of funds on behalf of, an Iranian-linked financial institution designated under the International Emergency Economic Powers Act (IEEPA); and whether the foreign bank has processed transfers of funds for the IRGC or any of its agents or affiliates designated under IEEPA.

Suspicious Activity Reporting

A financial institution may be required to tell a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or a empts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, which may include sanctions evasion.

The diagram below depicts this type of exchange house-related scheme:



Cyber Incident Preparedness Checklist

Before a Cyber Attack or Intrusion

- Identify mission critical data and assets (i.e., your "Crown Jewels") and institute tiered security measures to appropriately protect those assets.
- Review and adopt risk management practices found in guidance such as the National Institute of Standards and Technology Cybersecurity Framework.
- Create an actionable incident response plan.

o Test plan with exercises
o Keep plan up-to-date to reflect changes in personnel and structure

- Have the technology in place (or ensure that it is easily obtainable) that will be used to address an incident.
- Have procedures in place that will permit lawful network monitoring.
- Have legal counsel that is familiar with legal issues associated with cyber incidents
- Align other policies (e.g., human resources and personnel policies) with your incident response plan.
- Develop proactive relationships with relevant law enforcement agencies, outside counsel, public relations firms, and investigative and cybersecurity firms that you may require in the event of an incident.

During a Cyber Attack or Intrusion

- Make an initial assessment of the scope and nature of the incident, particularly whether it is a malicious act or a technological glitch.
- Minimize continuing damage consistent with your cyber incident response plan.
- Collect and preserve data related to the incident.

o "Image" the network
o Keep all logs, notes, and other records o Keep records of ongoing attacks

- Consistent with your incident response plan, notify—

o Appropriate management and personnel within the victim organization should o Law enforcement
o Other possible victims
o Department of Homeland Security

- Do not—

o Use compromised systems to communicate.
o "Hack back" or intrude upon another network.

After Recovering from a Cyber Attack or Intrusion

- Continue monitoring the network for any anomalous activity to make sure the intruder has been expelled and you have regained control of your network.
- Conduct a post-incident review to identify deficiencies in planning and execution of your incident response plan.

Justice Department Requires UTC to Divest Two Aerospace Businesses to Proceed With Acquisition of Rockwell Collins

The Department of Justice announced today that it will require United Technologies Corporation (UTC) to divest two businesses critical to the safe operation of aircraft to proceed with its acquisition of Rockwell Collins. First, UTC will divest Rockwell Collins's pneumatic ice protection systems business. Pneumatic ice protection systems remove ice from the wing of an aircraft by means of an inflatable rubber de-icing boot. Second, UTC will divest Rockwell Collins's trimmable horizontal stabilizer actuators (THSAs) business. THSAs ensure that an aircraft maintains altitude during flight by adjusting the angle of the horizontal tail surface.

"Today's remedy ensures that customers continue to benefit from competition in the supply of these two aircraft components that are critical to safety," said Assistant Attorney General Makan Delrahim of the Antitrust Division. "The remedy allows the divestiture buyers to compete vigorously to provide high quality systems and service to customers." The Department's Antitrust Division today filed a civil antitrust lawsuit today in the U.S. District Court for the District of Columbia to enjoin the proposed acquisition, along with a proposed settlement that, if approved by the court, would resolve the competitive concerns alleged in the lawsuit.

The Department said that, without the divestitures, the proposed acquisition would lessen competition substantially in the market for ice protection systems, by combining two of the world's three suppliers of pneumatic ice protection systems, and in the market for THSAs, by combining two of the world's leading producers of THSAs.

Under the terms of the proposed settlement, UTC must divest Rockwell Collins's ice protection systems business to an acquirer approved by the United States. UTC also must divest Rockwell Collins's THSA business to Safran S.A., an established aerospace supplier, or an alternate acquirer approved by the United States. The Antitrust Division, the European Commission, and the Competition Bureau of Canada cooperated closely throughout the course of their respective investigations. UTC is incorporated in Delaware and has its headquarters in Farmington, Connecticut. UTC produces a wide range of products for the aerospace industry and other industries. In 2017, UTC had revenues of approximately $59.8 billion.

Rockwell Collins is incorporated in Delaware and is headquartered in Cedar Rapids, Iowa. Rockwell Collins is a major provider of aerospace and defense electronics systems. In 2017, Rockwell Collins had revenues of approximately $6.8 billion.

Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading U.S. Aviation Companies

A Chinese Ministry of State Security (MSS) operative, Yanjun Xu, aka Qu Hui, aka Zhang Hui, has been arrested and charged with conspiring and attempting to commit economic espionage and steal trade secrets from multiple U.S. aviation and aerospace companies. Xu was extradited to the United States yesterday.

The charges were announced today by Assistant Attorney General for National Security John C. Demers, U.S. Attorney for the Southern District of Ohio Benjamin C. Glassman, Assistant Director Bill Priestap of the FBI's Counterintelligence Division, and Special Agent in Charge Angela L. Byers of the FBI's Cincinnati Division.

"This indictment alleges that a Chinese intelligence officer sought to steal trade secrets and other sensitive information from an American company that leads the way in aerospace," said Assistant Attorney General Demers. "This case is not an isolated incident. It is part of an overall economic policy of developing China at American expense. We cannot tolerate a nation's stealing our firepower and the fruits of our brainpower. We will not tolerate a nation that reaps what it does not sow."

"Innovation in aviation has been a hallmark of life and industry in the United States since the Wright brothers first designed gliders in Dayton more than a century ago," said U.S. Attorney Glassman. "U.S. aerospace companies invest decades of time and billions of dollars in research. This is the American way. In contrast, according to the indictment, a Chinese intelligence officer tried to acquire that same, hard-earned innovation through theft. This case shows that federal law enforcement authorities can not only detect and disrupt such espionage, but can also catch its perpetrators. The defendant will now face trial in federal court in Cincinnati."

"This unprecedented extradition of a Chinese intelligence officer exposes the Chinese government's direct oversight of economic espionage against the United States," said Assistant Director Priestap.

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.

*(*Continued On The Following Column)*

According to the indictment:

Beginning in at least December 2013 and continuing until his arrest, Xu targeted certain companies inside and outside the United States that are recognized as leaders in the aviation field. This included GE Aviation. He 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.

***

An indictment is merely a formal charge that a defendant has committed a violation of criminal law and is not evidence of guilt. Every defendant is presumed innocent until, and unless, proven guilty.

The maximum statutory penalty for conspiracy and attempt to commit economic espionage is 15 years of incarceration. The maximum for conspiracy and attempt to commit theft of trade secrets is 10 years. The charges also carry potential financial penalties. The maximum statutory sentence is prescribed by Congress and is provided here for informational purposes. If convicted of any offense, a defendant's sentence will be determined by the court based on the advisory Sentencing Guidelines and other statutory factors.

This investigation was conducted by the FBI's Cincinnati Division, and substantial support was provided by the FBI Legal Attaché's Office in Brussels. The Justice Department's Office of International Affairs provided significant assistance in obtaining and coordinating the extradition of Xu, and Belgian authorities provided significant assistance in securing the arrest and facilitating the surrender of Xu from Belgium.

Assistant Attorney General Demers and U.S. Attorney Glassman commended the investigation of this case by the FBI and the assistance of the Belgian authorities in the arrest and extradition of Xu. Mr. Demers and Mr. Glassman also commended the cooperation of GE Aviation throughout this investigation. The cooperation and GE Aviation's internal controls protected GE Aviation's proprietary information.

The case is being prosecuted by Assistant U.S. Attorneys Timothy S. Mangan and Emily N. Glatfelter of the Southern District of Ohio, and Trial Attorneys Thea D. R. Kendler and Amy E. Larson of the National Security Division's Counterintelligence and Export Control Section.

Protections
How to Protect Your Computer

Below are some key steps to protecting your computer from intrusion:

Keep Your Firewall Turned On: A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

Install or Update Your Antivirus Software: Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

Install or Update Your Antispyware Technology: Spyware is just what it sounds like—software that is surreptitiously installed on your computer to let others peer into your activities on the computer. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your web browser. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable antispyware—in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries—shop where you trust.

Keep Your Operating System Up to Date: Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

Be Careful What You Download: Carelessly downloading e-mail attachments can circumvent even the most vigilant anti-virus software. Never open an e-mail attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly advanced malicious code.

Turn Off Your Computer: With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection, which is designed to fend off unwanted attacks, turning the computer off effectively severs an attacker's connection—be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

Texas Resident Sentenced in South Florida to More Than 6 Years in Prison for Violations of the Cuban Embargo

On September 27, 2018, a Texas resident was sentenced in the Southern District of Florida to 6.5 years in prison for unlawfully exporting to Cuba electronic devices that require a license to export due to national security controls.

Ariana Fajardo Orshan, United States Attorney for the Southern District of Florida, Robert J. Luzzi, Special Agent in Charge, U.S. Department of Commerce Office of Export Enforcement (OEE), Miami Field Office, Mark Selby, Special Agent in Charge, U.S. Immigration and Customs Enforcement's Homeland Security Investigations (ICE-HSI), Miami Field Office, and Diane J. Sabatino, Director, Field Operation, U.S. Customs and Border Protection (CBP), Miami Field Office made the announcement.

Bryan Evan Singer, 46, of Bryan, Texas was convicted at trial for attempting to illegally smuggle electronics to Cuba in violation of the Cuban Embargo, in violation of Title 18, United States Code, Section 554, and for making false statements to federal law enforcement, in violation of Title 18, United States Code, Section 1001(a)(2). On September 27, 2018, 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 their capabilities threaten national security. Singer never sought or obtained a license to export to Cuba, prior to his offenses of conviction. U.S. Attorney Fajardo Orshan commended the investigative efforts of OEE, ICE-HSI, and CBP in this matter. Mrs. Fajardo Orshan thanked the U.S. Coast Guard for the agency's assistance. This case was prosecuted by Assistant U.S. Attorney Brian J. Shack.

Related court documents and information can be found on the District Court for the Southern District of Florida's website at http://www.flsd.uscourts.gov/or on http://pacer.flsd.uscourts.gov./

Training

There is still time to register for the upcoming Bureau of Industry and Security seminars in New Orleans, including the comprehensive 2-day Complying with U.S. Export Controls, and the 1-day How to Build an Export Compliance Program:

■ Complying with U.S. Export Controls – 2 Days
October 23-24, 2018
New Orleans, LA

This two-day program is led by BIS's professional counseling staff and provides an in-depth examination of the EAR. The program will cover the information exporters need to know to comply with U.S. export control requirements on commercial goods. We will focus on what items and activities are subject to the EAR, steps to take to determine the export licensing requirements for your item, how to determine your export control classification number (ECCN), when you can export or reexport without applying for a license, export clearance procedures and record keeping requirements, and real life examples in applying this information. Presenters will conduct a number of "hands-on" exercises that will prepare you to apply the regulations to your own company's export activities.

For registration, CLICK HERE

■ How to Build an Export Compliance Program – 1 Day
October 25, 2018
New Orleans, LA

How to Build an Export Compliance Program is a one-day workshop that provides an overview of the steps a company may take to implement an internal Export Compliance Program. Developing and maintaining an export compliance program is highly recommended to ensure that export transactions comply with the EAR, and to prevent export control violations. Agenda topics include guidance on how to establish an Export Compliance Program, strategies to enhance your company's compliance program, how to avoid common compliance errors, and how to build a solid framework for your company's compliance program.

*(*Continued On The Following Column)*

This program includes small group discussion, hands-on exercises, compliance peer networking, and provides a written example of an export compliance program as well as the Office of Exporter Services January, 2017 revised Export Compliance Guidelines to assist in developing your compliance program. Recommended prerequisite: Essentials of U.S. Export Controls or Complying with U.S. Export Controls or equivalent experience.

For registration, CLICK HERE

BIS Annual Conference 2019 Suggestion Form

This form is provided for the exclusive purpose of allowing users to submit topic, content, or format suggestions to BIS for the 2019 Annual Conference.

The Bureau of Industry and Security, Office of Exporter Services, is preparing for the 2019 Annual Conference on Export Controls and Policy. We hope to host the conference in late spring or early summer but do not have firm dates yet. We are in the process of developing a proposed agenda, and would like to solicit your input. We invite you to provide your recommendations regarding content or format for 2019's conference agenda, breakout sessions, plenary sessions, special workshops or forums, and roundtable discussion topics. If you recommend a topic, please also identify any relevant agencies you would like to see invited, and/or appropriate panel moderators and speakers.

We would appreciate your input as soon as possible. To refresh your memory about last year's topics and speakers, you may view the 2018 Annual Conference materials on our website at:
https://www.bis.doc.gov/index.php/compliance-a-training/export-administration-regulations-training/annual-conference-2018

To make suggestions, see link:
https://www.bis.doc.gov/index.php/component/rsform/form/41-bis-annual-conference-2019-suggestion-form

EIB World Trade Headlines
Evolutions In Business • www.eib.com • (978) 256-0438 • P.O. Box 4008, Chelmsford, MA 01824