

International Trade Enforcement Roundup

BASS
BERRY
SIMS

You are reading Bass, Berry, & Sims' new enforcement roundup, where we bring notable enforcement actions, policy changes, interesting news articles, and a bit of our insight to your inbox every month.

To stay up to date, subscribe to our [GovCon & Trade blog](#). If you have questions about any of the actions mentioned and how they relate to your business, contact our firm's international trade team. We welcome your feedback and encourage sharing this newsletter with anyone interested.

Following an active October, enforcement actions and regulatory policy changes slowed in November. With that said, the actions taken in November involved some novel topics and provide several insights to glean.

Overview

- ◆ November was another busy month for **China-specific actions**. Three Kentucky natives were indicted for exporting technical data without a license and violating the Defense Acquisition Regulations System (DFARS) specialty metal clause, and face significant jail time. Additionally, in an unprecedented case, the Department of Justice (DOJ) convicted a Chinese economic spy for attempting to steal trade secrets from GE Aviation. Across the pond, the United Kingdom forced the sale of a Chinese company's majority interest in the UK's largest semiconductor manufacturing facility.
- ◆ The Department of Commerce's Bureau of Industry and Security (DOC/BIS) took separate actions against an American and an Iranian for illegally exporting controlled items into **Iran**. Both used the United Arab Emirates (UAE) as a transshipment point. Additionally, a Temporary Denial Order (TDO) was renewed against Mahan Airlines (of Iran) and a number of related parties.
- ◆ The TDO covering Rossiya Airlines (Russia) was renewed for the airline's continued operation in violation of the Export Administration Regulations (EAR). Otherwise, things were slower last month for **Russia-related enforcement actions**. That doesn't mean U.S.-origin products aren't making it onto the battlefield in Ukraine. According to a November 16, 2022, Wall Street Journal article, a downed Iranian Mohajer-6 drone revealed that parts produced by U.S. firms accounted for 50% of the drone's total components. While enforcement actions usually lag BIS discoveries, expect more enforcement actions to come.
- ◆ Another action taken against a well-known **cryptocurrency** company demonstrates the Treasury Department's Office of Foreign Asset Control's (OFAC) eagerness to bring the industry to heel. The company - Kraken - agreed to pay over \$350,000 in penalties.

China

Three Arrested for Illegal Scheme to Export Controlled Data and Defraud the Department of Defense (DOJ Action)

Those involved. Phil Pascoe; Monica Pascoe; Scott Tubbs; and Quadrant Magnetics, a U.S.-based provider of magnets and magnetic-based materials.

Charges with penalties. Wire Fraud (maximum of 20 years); Exporting Technical Data without a license (maximum of 20 years); Smuggling Goods out of the United States (10 years); and Conspiracy to Defraud the United States (5 years).

What happened? On November 9, Phil Pascoe, Monica Pascoe, and Scott Tubbs were indicted. The DOJ alleges the defendants conspired to send to China dozens of technical data drawings controlled under the International Traffic in Arms (ITAR). The drawings, which were sent as attachments to emails, related to submarine periscopes, multi-spectral targeting systems, infrared imaging systems, and the F-16 radar. The United States maintains an absolute embargo on ITAR exports to China.

In addition, [the indictment](#) alleges that Quadrant Magnetics imported and sold magnets from China to two U.S. government contractors but misrepresented that the items were magnetized in Louisville, Kentucky. Those magnets were then included in products sold to the Department of Defense in violation of the DFARS specialty metal clause.

Read the press release [here](#).

Notably. Companies doing business with China should know that exports do not require physical objects moving across borders. As was the case here, emailing attachments containing technical data covered by the ITAR can result in criminal penalties.

Moreover, companies doing business with the government should understand that DFARS requirements apply to subcontractors. Here, DFARS 225.252-7009, the specialty magnets clause, applied to Quadrant Magnetics just as it applied to the prime contractor.

Chinese Government Intelligence Officer Sentenced to 20 Years in Prison for Espionage Crimes, Attempting to Steal Trade Secrets from Cincinnati Company (DOJ Action)

Those involved. Yanjun Xu, Deputy Division Director of China's Ministry of State Security (MSS), a Chinese intelligence agency responsible for counterintelligence, foreign intelligence and political security.

Charges with penalties. Conspiracy to Commit Economic Espionage; Conspiracy to Commit Trade Secret Theft; Attempting Economic Espionage by Theft or Fraud. Xu was convicted of two counts of conspiracy and attempting to commit economic espionage and two counts of attempting to steal trade secrets. He was sentenced to 20 years in prison.

What happened? Xu, acting undercover, worked with a General Electric (GE) Aviation employee to attempt to obtain technical information related to GE Aviation's fan blades and relay it to the Chinese government. Xu, presenting himself as a Jiangsu Science and Technology Association (JSTA) representative, lured the GE employee into giving a presentation about his work and offered to pay his expenses. After the trip, Xu continued to communicate with the GE employee and asked the employee several questions related to the fan blades.

After the employee sent a document marked “trade secret,” Xu and the employee made plans to meet in Belgium to discuss further. Ultimately, the GE employee disclosed the events to his employer, who engaged the FBI. In Belgium, Xu was arrested as part of a sting operation and extradited to the United States to stand trial.

Prosecutors stated that Xu’s activities are part of a broader Chinese policy to “reinnovate” foreign technologies by obtaining trade secrets from non-Chinese aviation companies. In this regard, prosecutors cited an attempt by Xu to leverage “insiders” at a French engine manufacturer and place malware on company computers to infiltrate the company network.

Notably. U.S. government agencies continue to warn American companies about Chinese economic espionage efforts. The indictment gives us a behind-the-curtain look into what Chinese tactics look like and offers clues for how (i.e., training personnel) companies should protect against illegal exports of data.

Read the press release [here](#).

Nexperia Ordered to Sell its Controlling Stake in UK’s Largest Semiconductor Factory (UK Department of Business, Energy, and Industrial Strategy Action)

Those involved. Nexperia BV, a Dutch-headquartered semiconductor manufacturer and subsidiary of Wingtech Technology, a Chinese state-owned communication equipment manufacturer.

Action. The forced sale of 86% of Nexperia’s share capital in Newport Water Fab.

What happened? On July 5, 2021, Nexperia bought 86% of the share capital in Newport Wafer Fab, giving the company 100% ownership of the semiconductor production facility. Following legislation that came into effect earlier in 2022, the UK government took a second look at the acquisition. The decision followed an assessment concluding that the sale presented risks to UK national security given the potential loss of UK technological capabilities.

Read the publication of notice of final order [here](#). Read the Reuters article [here](#).

Notably. The U.S. government has promoted a new national security strategy toward China founded on technological leadership and modern industrial policy. While the U.S. has pressed ahead with technological investments and strengthened inbound investment screening parameters, the question remains whether allies would come aboard. Recently, allies (namely the Dutch) have expressed concern about aligning export controls; however, the recent UK order and a similar German action blocking a Chinese acquisition of a German semiconductor company may indicate an increased appetite for the heightened scrutiny of the inbound investment prong of the U.S. effort.

Iran

Alabama Man Indicted for Violating U.S. Sanctions Against Iran (DOJ Action)

Those involved. Ray Hunt

Charges and penalties. Unlawful Export of U.S.-Origin Goods to Iran (maximum of 20 years in prison and up to a \$1 million fine); Conspiracy (maximum of five years in prison); Smuggling Goods from the United States (maximum of 10 years); Submitting False or Misleading Export Information (maximum of 10 years).

What happened? Ray Hunt, an Iranian-born U.S. citizen living in Alabama, was charged after exporting U.S.-controlled items used in the oil and gas industry to Iran. Hunt used his company, Vega Tools LLC, to buy valves, tubing, and other items from American producers and resell them to Iranian companies using the UAE and Turkey as transshipment points. Hunt also falsified his export records to deceive shipping companies about the ultimate destination and value of the goods.

Read the indictment [here](#). Read the press release [here](#).

Notably. The indictment shows that the UAE remains a preferred transshipment point for U.S.-origin products destined for Iran (and Syria). The UAE is also a common transshipment point for controlled exports bound for Russia or Belarus, according to an [August BIS FAQ](#).

BIS Issues Charging Letter Against Mohammad Alhamra and WEBS Electronics Trading Company for Violating U.S. Export Controls (DOC/BIS Action)

Those involved. Mohammad Alhamra; WEBS Electronic Trading Company, a UAE-based trading company.

Charges with penalties. Solicitation and Attempt; Engaging in Prohibited Conduct by Re-exporting Controlled Items to Syria without BIS Authorization; Engaging in Prohibited Conduct by Re-exporting Controlled Items to Iran without BIS Authorization; Misrepresenting and Concealing Facts to an Official of a United States Agency (up to \$330,947 in penalties per violation or twice the value of the transaction and denial of export privileges).

What happened? In April 2018, a BIS Export Control Officer (ECO) became aware that WEBS was attempting to re-export a U.S.-origin switch and transceiver from the UAE to Syria. During a post-shipment verification (PSV), Alhamra denied selling to Syria. A month later, the ECO became aware of another attempt to re-export U.S.-origin technology to Syria and conducted another PSV. This time, Alhamra admitted that up to 80% of WEBS sales were to Syria. Upon further investigation, BIS found that Alhamra had re-exported U.S.-origin items numerous times to a company in Syria and a customer in Iran.

Read the charging letter [here](#). Read the press release [here](#).

Notably. Non-U.S. companies must comply with the same U.S. export control laws that U.S. companies comply with when exporting U.S.-origin products. Re-exporting U.S.-origin products, even EAR99 products, to either Syria or Iran requires a BIS license in nearly every case.

Iranian Airlines - Temporary Denial Orders (DOC/BIS Action)

On November 8, BIS [renewed](#) a previously issued TDO against Mahan Airways (Mahan), Pejman Mahmood Kosarayanifard, Mahmoud Amini, Kerman Aviation, Sirjanco Trading LLC, Mahan Air General Trading LLC, Mehdi Bahrami, Al Naser Airlines, Ali Abdullah Alhay, Bahar Safwa General Trading, Sky Blue Bird Group, and Issam Shammout. BIS cited Mahan's continued operation in violation of the May 13, 2022 TDO and the EAR: Mahan re-exported an aircraft, obtained through Al Naser Airlines, to Russia without a license and continues to operate three unauthorized aircraft between Russia, Iran, and the UAE.

The Federal Register notice can be found [here](#).

Russia

Russia Airlines - Temporary Denial Orders (DOC/BIS Action)

On November 15, BIS [renewed](#) a previously issued TDO against Rossiya Airlines, citing the airline's continued operation in violation of the May 20, 2022 TDO and the EAR. In particular, according to BIS, the airline operates multiple aircraft into Russia in violation of the EAR, including flights from Antalya and Istanbul, Turkey. The renewal of the TDO means that Rossiya continues to be banned from participating in transactions subject to the EAR, including exports from the United States and re-exports abroad.

Cryptocurrency

OFAC Settles with Virtual Currency Exchange Kraken for \$362,158.70 for Apparent Violations of the Iranian Transactions and Sanctions Regulations (OFAC Action)

Those involved. Payward, Inc. (Kraken), a virtual currency exchange based in Delaware.

Charges with penalties. 826 violations of the Iranian Transactions and Sanctions Regulations. Kraken agreed to pay over \$362,000 in penalties. The maximum applicable civil penalty was over \$270,000,000.

What happened? Kraken, the second-largest U.S. cryptocurrency exchange by volume, agreed to pay over \$362,000 in penalties after voluntarily disclosing to the OFAC that it had processed 826 transactions amounting to roughly \$1,680,000 for individuals located in Iran. The penalty is the conclusion of an OFAC investigation which the New York Times [reported](#) began in 2019. While Kraken vetted customer locations at the time of account sign up, the company failed to conduct another location check at the time of sign-in. OFAC stated, "the settlement amount reflects [the agency's] determination that Kraken's apparent violations were non-egregious and voluntarily self-disclosed." OFAC credited Kraken for its voluntary disclosure, a prior clean record, a new "dedicated head of sanctions," and for investing \$100,000 into a number of remedial measures, including compliance training for staff and geolocation blocking.

Read the enforcement notice [here](#).

Notably. This action is just the latest in a series of settlements among companies in the cryptocurrency industry. Last month, Bittrex [agreed](#) to the largest monetary settlement by a crypto company to date when it agreed to pay over \$24 million for sanctions violations. Earlier in the year, OFAC sanctioned [Tornado Cash](#). As the FTX fallout deepens and public perception of the industry darkens, virtual currency companies should ensure they have implemented the proper compliance infrastructure to ensure they do not violate sanctions.

Enforcement Policy Updates

There were no new enforcement policy updates in November.

Please contact the authors if you have any questions about these enforcement updates and how they may impact your business.

International Trade Team

The Bass, Berry & Sims International Trade Practice Group helps clients navigate the complex regulations associated with a global marketplace. Our team is experienced in guiding clients through challenging issues related to economic sanctions (OFAC), exports (DDTC and the ITAR; BIS and the EAR), imports (CBP), anti-bribery (DOJ and SEC), anti-boycott regulations (OAC and Treasury), and the Committee on Foreign Investment in the United States (CFIUS). Our work in this area has been recognized in leading legal industry outlets, including Chambers USA, whose research revealed “Bass, Berry & Sims represents a range of clients in export controls and economic sanctions matters. The team is experienced in handling EAR, OFAC and ITAR issues.” A client added, “Bass, Berry & Sims is very responsive and service-oriented.” (from Chambers USA 2022). Learn more [here](#).



[Mi-Yong Kim](#)

(202) 827-2970

miyong.kim@bassberry.com



[Thaddeus R. McBride](#)

(202) 827-2959

tmcbride@bassberry.com



[Sylvia Yi](#)

(202) 827-2993

syi@bassberry.com