International Trade
Enforcement Roundup

BASS BERRY SIMS

You are reading the **February 2024 Update** of the Bass, Berry & Sims Enforcement Roundup, where we bring notable enforcement actions, policy changes, interesting news articles, and a bit of our insight to your inbox.

To stay up to date, subscribe to our GovCon & Trade blog. If you have questions about any actions addressed in the Roundup, please contact the international trade team. We welcome your feedback and encourage you to share this newsletter. Let's get into it!

Overview

- February saw a continuing focus on **Russia**. First, the Treasury Department's Office of Foreign Assets Control (OFAC), in conjunction with the State Department, sanctioned over 500 individuals and entities – the "largest number of sanctions imposed since Russia's full-scale invasion of Ukraine." The Commerce Department's Bureau of Industry and Security (BIS) also added 93 entities to its Entity List. Second, the Department of Justice (DOJ) disrupted two separate sanctions evasion schemes with individuals entering guilty pleas.

- There were three notable actions involving **Iran** this month. BIS reached an administrative settlement with CargoSave, a freight shipper, which seems to have been granted "credit" for assisting in an investigation of a third party. Also, a UK citizen was sentenced to 18 months in prison for conspiring to export U.S.-origin goods to Iran, and a father-son duo was charged with facilitating the export of a variety of U.S.-origin equipment and technology to Iran.

- February also saw a flurry of enforcement actions involving **China**. Boeing agreed to settle 199 Violations of the International Traffic in Arms Regulations (ITAR) when it allowed foreign person employees (FPEs), some residing in China, access to ITAR-controlled files on an internal server. And a U.S. citizen pleaded guilty to conspiring to commit wire fraud after he sourced parts and components from China in violation of contracts with the U.S. government.

Russia

U.S. Government Sanctions Hundreds of Targets in Russia and Globally (OFAC, BIS, Department of State Action)

Navalny + Two Year Anniversary. On February 23, in conjunction with the State Department, OFAC sanctioned over 500 individuals and entities in what amounted to the "largest number of sanctions imposed since Russia's full-scale invasion of Ukraine." OFAC targeted Russia's financial infrastructure, third-country sanctions evaders, and various other entities supporting the Russian military-industrial base as well as other sectors of the Russian economy. All transactions by U.S. persons involving the property of the designated entities are prohibited, and U.S. persons holding property of any of these entities must block and report that property to OFAC.

BIS also added 93 entities to the Entity List. Most of the entities are based in Russia, while the remainder are in China, India, Kyrgyzstan, South Korea, Turkey, and the United Arab Emirates (UAE). As a general matter, a license is required to export, re-export, or transfer nearly any U.S.-origin item to a party on the Entity List.

The OFAC press release can be found here. The Department of State press release can be found here. The Department of Commerce press release can be found here.

Notably. The new designations heighten the risk of doing business in or involving Russia. Designations can be made with little or no warning and can immediately disrupt previously permissible business. Companies must review additions and adapt compliance systems where appropriate.

Russian International Pleads Guilty to Illicitly Procuring Military Grade Microelectronics for Russian Entities (BIS Action)

Those involved. Maxim Marchenko, a Russian citizen.

Charges with penalties. One Count of Money Laundering (maximum of 20 years in prison); One Count of Smuggling Goods from the United States (maximum penalty of 10 years).

What happened? On February 29, Marchenko pleaded guilty to charges arising from an illicit procurement network operating across Russia, Hong Kong, and elsewhere. The network fraudulently obtained dual-use, military-grade microelectronics from U.S. suppliers. Marchenko used several Hong Kong-based shell companies to conceal the fact that Russia was the ultimate destination for the items. Marchenko told U.S. suppliers that the components would be sent to China, Hong Kong, and other countries outside of Russia. He is scheduled to be sentenced on May 29. We wrote about the September 2023 indictment here.

The press release can be found here.

Notably. This enforcement action reinforces the fact that Hong Kong is a common transshipment point for U.S.-origin products bound to Russia. Due diligence on transactions transiting Hong Kong, especially those involving sensitive electronics, needs to be carefully reviewed for compliance red flags that could evidence risk of diversion or other improper use.

Russian-Canadian National Pleads Guilty to Money Laundering as part of Conspiracy to Send Weapons Components to Russia in Violation of U.S. Sanctions (DOJ Action)

Those involved. Kristina Puzyreva, a Russian national residing in Canada.

Charges with penalties. One Count of Conspiracy to Commit Money Laundering (maximum of 20 years in prison).

What happened? On February 12, Puzyreva pleaded guilty to money laundering conspiracy for her role in a larger procurement scheme attempting to export certain components for use in Russian weapons systems. The scheme, involving two Brooklyn companies—SH Brothers and SN Electronics—and at least six other individuals, shipped millions of dollars in U.S.-origin components to sanctioned entities in Russia. Components were bought from U.S. companies, shipped to various addresses in Brooklyn, then repackaged and exported using various intermediary countries like China, including Hong Kong, India, Turkey, the UAE, and others. These components were subsequently found in Russian unmanned aerial vehicles (UAVs) and guided missiles in Ukraine.

The press release can be found here.

Notably. The indictment and plea highlight the potentially lucrative nature of these types of procurement schemes. In one message, Puzyreva emphasized that she and the co-conspirators would "get rich." Such monetary inducements make it likely that such schemes will continue.

Iran

BIS Slaps Freight Company on Wrist for Facilitating Iran Exports (BIS Action)

Those involved. Cargosave, Inc., a New York-based freight shipper.

Charges with penalties. Two Charges of Causing, Aiding, or Abetting a Violation (agreed to a suspended 2-year denial order).

What happened? On February 12, Cargosave agreed to an administrative enforcement settlement after it facilitated the unauthorized export of enterprise servers and switches—items controlled under the EAR and Iranian Transactions and Sanctions Regulations (ITSR)—to Iran on behalf of an Iranian exporter. BIS did not impose a financial penalty on Cargosave after considering the company's cooperation with the investigation and assistance Cargosave provided in a separate investigation related to a third party. In determining that no monetary penalty was warranted, BIS took into account Cargosave's admission that it committed the alleged conduct and its agreement to conduct compliance training.

Notably. A January 2023 update to BIS's Voluntary Self-Disclosure (VSD) process emphasizes that parties can get favorable treatment in any concurrent or future enforcement action by providing information about violations committed by others. BIS seems to have given Cargosave "credit" for assisting in a separate investigation related to a third party. We wrote about the VSD update here.

In addition, this enforcement action punctuates a recent BIS effort to target freight forwarders. In December 2023, the Departments of Commerce, Treasury, Justice, State, and Homeland Security (DHS) published a quint-seal compliance note summarizing trade compliance best practices for freight shippers and the necessity that they "know [their] cargo."

UK Citizen Sentenced to Prison for Attempting to Export U.S. Technology to Iran (DOJ Action)

Those involved. Saber Fakih, a United Kingdom (UK) citizen.

Charges with penalties. Violating Count Two of the Indictment—Violating the International Emergency Economic Powers Act (IEEPA) (sentenced to 18 months in prison).

What happened? On February 1, Fakih was sentenced to 18 months in prison after pleading guilty to violating the IEEPA. According to the plea agreement, Fakih and several co-conspirators worked to export an Industrial Microwave System (IMS) and a counter-drone system from the United States to Iran without the necessary OFAC license. Both items had potential military uses. Fakih apparently acted as a middleman for the Iranian purchaser and the U.S. sellers and understood the items would eventually be exported to Iran. Fakih was arrested in the UK in February 2021 and entered a plea on January 25, 2022.

The press release can be found here.

Notably. The DOJ continues to aggressively pursue enforcement actions against individuals; this is yet another example of that trend, which we expect to continue.

DOJ Announces Charges and Arrest in Illicit Technology Transfer Schemes to Benefit Governments of Iran and China (DOJ Action)

United States v. Bazzazi

Those involved. Abolfazi Bazzazi and Mohammad Resa Bazzazi, Iranian nationals.

Charges with penalties. Conspiracy to Violate the IEEPA (maximum 20 years in prison) and Smuggling Goods from the United States (maximum 10 years in prison).

What happened? On February 7, the DOJ unsealed an indictment alleging the Bazzazis—a father-son duo—"devised an intricate scheme to evade U.S. export laws in obtaining U.S. equipment and technology to be exported to Iran and for the Government of Iran." Between January 2008 and August 2019, the Bazzazis allegedly procured "aeronautical ground support equipment, UV-detectors and firefighting equipment, parts and technology" for export to Iran and to the Government of Iran without authorization. They allegedly caused U.S. sellers to export the goods, concealing the ultimate destination by attempting to forward the goods through European intermediaries. The defendants remain at large.

United States v. Gong

Those involved. Chenguang Gong, a U.S. citizen and Chinese native.

Charges with penalties. Theft of Trade Secrets (maximum of ten years in prison).

What happened? On February 6, Gong was arrested and charged with theft of trade secrets after allegedly transferring to his personal devices over 3,600 files belonging to his employer, an unnamed company that apparently worked alongside the Defense Department to develop advanced sensors and circuitry for "space-based missile warning and tracking, space-based surveillance, and airborne infrared countermeasures systems."

The FBI also discovered that Gong had "submitted numerous applications to 'Talent Programs' administered by the People's Republic of China." Such programs apparently exist to "identif[y] individuals located outside the PRC who have expert skills, abilities, and knowledge that would aid in transforming the PRC's economy, including its military capabilities." In his applications, Gong proposed to develop certain sensors and technologies that mirrored the ones he had been working on at his unnamed employer. Gong was arrested in San Jose on February 6.

The press release can be found here.

Notably. These cases were announced to mark the one-year anniversary of the launch of the Disruptive Technology Strike Force, which brings together representatives from BIS, DOJ, FBI, DHS, and multiple U.S. attorney's offices and coordinates with international partners to bring export enforcement actions.

China

Boeing, State Department Reach $51 Million Settlement to Resolve Export Violations (Department of State Action)

Those involved. The Boeing Company, a global aerospace giant.

Charges with penalties. 199 Violations of the Arms Export Control Act (AECA) and the ITAR (civil penalty of $51 million).

What happened? On February 19, the State Department's Directorate of Defense Controls (DDTC) reached a settlement with Boeing to resolve almost 200 violations of the AECA and ITAR. A majority of the violations arose from foreign-person employees (FPEs) at overseas facilities downloading ITAR-controlled technical data from Boeing's digital document repository. Downloaded data related to a variety of high-profile weapons systems, including the F-18, F-22, AH-64 Apache Helicopter, and AGM-84E Standoff Land Attack Missile. Boeing also exported technical data without the required authorization due to jurisdiction and classification issues, and failure to comply with terms and conditions of DDTC authorizations.

In determining the penalty to impose, DDTC considered as mitigating factors Boeing's voluntary disclosure in the matter, the fact that many violations predated several improvements Boeing made to its compliance program, and Boeing's considerable cooperation with DDTC, including the company's agreement to toll the statutory limitations period. DDTC likewise considered as aggravating factors the harm to U.S. national security, especially the fact that unauthorized exports were made to China and Russia, and the breadth of violations across multiple business units and subsidiaries. As a condition of the settlement, Boeing must also undergo two audits conducted by an outside consultant. The government also agreed to suspend $24 million of the penalty if Boeing uses the money to strengthen its existing compliance program.

The press release can be found here.

Notably. The action highlights that even the largest and most sophisticated companies, with extensive international experience, can fall afoul of the complicated U.S. export regulations. For companies like Boeing with operations and personnel around the world, it is particularly important to maintain controls on access to technical data given that personnel are based or may travel to many countries for which an export license is required.

Missouri-Based Defense Contractor Commits Fraud (DOJ Action)

Those involved. David Maurar, a U.S. citizen.

Charges with penalties. One Count of Conspiracy to Commit Wire Fraud (maximum of 20 years in prison, a fine of up to $250,000, or both).

What happened? On February 7, the DOJ announced that Maurar had pleaded guilty to one count of conspiracy to commit wire fraud arising from a scheme to win government contracts by making misrepresentations about the sources of specific parts. Although he had contracted with the government to only provide parts of domestic origin, Maurer in fact fraudulently procured parts from China, including Hong Kong, and elsewhere. Maurar also sent diagrams of the parts to non-U.S. suppliers after removing export control warnings. Maurar is scheduled to be sentenced on May 7.

The press release can be found here.

Notably. Government contractors face additional avenues of liability that commercial companies may not. Many government contracts include domestic preference rules for items delivered to the government. Failure to comply with contractual obligations can lead to civil and criminal charges. With the Biden Administration prioritizing domestic preference programs through executive actions and legislation, similar violations will likely increase.

International Trade Practice Group

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), antibribery (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 that "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*).

Learn more here.

Authors

Faith Dibble
202-827-2965
faith.dibble@bassberry.com

Thaddeus R. McBride
202-827-2959
tmcbride@bassberry.com