SHEARMAN & STERLING

Sanctions Roundup

January 20, 2022

FOURTH QUARTER 2021

- President Biden signs Xinjiang forced labor legislation as US sanctions numerous Chinese tech firms for ties to PRC military, and further targets officials for undermining Hong Kong's autonomy.
- State Department sanctions firm involved in constructing Nord Stream 2 as concerns grow over another potential Russian invasion of Ukraine.
- EU's top court finds that EU operators may terminate Iran contracts if sanctions present "disproportionate economic consequences."
- US addresses human rights abuses and targets corrupt actors worldwide to coincide with US-led Summit for Democracy.
- US financial institution settles two actions for compliance failures associated with maintaining bank accounts for sanctioned customers.

CONTENTS

CHINA

For five years now, tough measures to combat perceived aggressions by the People's Republic of China have been a hallmark of US foreign policy, particularly PRC activities relating to democracy and human rights. This quarter, the Biden Administration resumed its campaign of sanctions measures, including by signing into law bipartisan legislation aimed at restricting the import of goods potentially connected to forced labor in Xinjiang. To curb the PRC's military modernization and development of surveillance technology, the Commerce Department blacklisted a host of Chinese tech firms. In related developments, the Treasury Department imposed restrictions on transactions in the publicly listed securities of Chinese tech firms by designating them as Chinese Military Industrial Complex Companies. Meanwhile, five PRC officials were sanctioned for allegedly implementing anti-democratic measures in Hong Kong, and the SEC implemented rules to increase oversight of foreign issuers.

President Biden Signs Xinjiang Forced Labor Legislation into Law

As the quarter closed, the Biden Administration's commitment to addressing alleged human rights abuses kept apace. On December 23, President Biden signed into law bipartisan legislation aimed at addressing reported abuses against the Uyghur Muslim population in the Xinjiang Uyghur Autonomous Region. Titled the "Uyghur Forced Labor Prevention Act," the Act aims to prohibit the importation into the United States of goods "mined, produced or manufactured wholly or in part with forced labor" from China, in particular from Xinjiang. The Act also imposes broad restrictions on the import of goods made of material sourced from Xinjiang or connected to persons working with the Xinjiang regional government or the Xinjiang Production and Construction Corps. The far-reaching scope of the Act means that the prohibitions apply to goods made by companies based outside of

Xinjiang, and even outside China, that source materials from Xinjiang or produce even a portion of the product inside of Xinjiang.

Goods meeting the above criteria will be presumed to be the product of forced labor and therefore denied entry into the United States. The Act provides a mechanism for companies to rebut the presumption of forced labor if an importer can demonstrate to US Customs and Border Protection the following:

- the goods were not produced wholly or in part by forced labor;
- the importer has complied with diligence requirements and effective supply chain management; and
- the importer has responded to all inquiries for information from CBP.

If CBP finds that an importer has furnished evidence sufficient to rebut the presumption, CBP must first issue a public report identifying the goods to be imported and the CBP's evidentiary findings and submit that report to Congress.

Before the law takes effect on June 21, 2022, the Act provides a 75-day window during which companies may submit comments to the newly-created Forced Labor Enforcement Task Force, comprised of representatives from the US Departments of Homeland Security, State, Justice, Commerce, Labor, and Treasury, as well as the US Trade Representative and the US Agency for International Development. The task force will then submit to Congress a report describing its enforcement strategy.

Commerce Department Blacklists Host of Chinese Companies for Military Ties

This quarter, the Bureau of Industry and Security at the US Department of Commerce issued of series of Entity List designations and export control restrictions to prevent the export to China of goods and technology related to artificial intelligence, quantum computing, biotechnology, and drone surveillance. On December 16, BIS announced that it would add thirty-seven companies to the Entity List, including a host of Chinese companies and research institutes for their alleged ties to Chinese military programs. Among the thirty-seven entities were Chinese firms **HMN International**, **Jiangsu Hengtong Marine Cable Systems**, **Jiangsu Hengtong OpticElectric**, **Shanghai Aoshi Control Technology Co. Ltd.**, and **Zhongtian Technology Submarine Cable**, which were added to the Entity List for alleged efforts to acquire US-origin items in support of Chinese military modernization. Also added to the Entity List was the **Academy of Military Medical Sciences**, based in China, and eleven of its research institutes. According to the Commerce Department, two of the Academy's research institutes use biotechnology processes to support the Chinese military and develop purported "brain-control" weaponry. In a statement, the Secretary of Commerce declared that the Department "cannot allow U.S. commodities, technologies, and software that support medical science and biotechnical innovation to be diverted toward uses contrary to U.S. national security."

The December 16 Entity List designations follow the addition in late November of twenty-seven Chinese and third-country entities for their role in "quantum computing efforts that support military applications, such as "counter-stealth and counter-submarine applications, and the ability to break encryption or develop unbreakable encryption," among other activities." The eight PRC-based technology entities added to the Entity List are alleged to have acquired US-origin electronic items to support the PRC's modernization of its military. The eight China-based firms include **Hefei National Laboratory for Physical Sciences at Microscale**, **QuantumCTek Co.**, **Shanghai QuantumCTeck Co., Ltd.**, **Hangzhou Zhongke Microelectronics Co., Ltd.**, **Hunan Goke Microelectronics**, **New H3C Semiconductor Technologies Co., Ltd.**, **Xi'an Aerospace Huaxun Technology**, and **Yunchip Microelectronics.**

Chinese Tech Firms Identified as Non-SDN CMICCs

In December, OFAC acted twice pursuant to E.O. 13959, as amended by E.O. 14032, to identify a total of nine Chinese technology firms as non-SDN Chinese Military Industrial Complex Companies (non-SDN CMICs) for their alleged connections to China's defense and surveillance technology sectors. In the first action, OFAC added **SenseTime Group Limited** for operating in the surveillance technology sector of the PRC's economy, particularly

its technology related to facial recognition programs allegedly used in the Xinjiang Uyghur Autonomous Region. While this designation did not directly target the SenseTime subsidiary that was in the process of an IPO, it nevertheless caused some disruption and delay to that process, although the company did eventually go through with the offering.

On December 16, OFAC designated an additional eight technology firms for allegedly assisting the PRC's reported surveillance and monitoring of minority populations in China, particularly those living in Xinjiang. The technologies of these firms, such as facial recognition software, computer tracking software, and surveillance drone technology, have been deployed in Xinjiang and across China to track the movements of ethnic minorities. The eight entities include **Cloudwalk Technology Co., Ltd.**; **Dawning Information Industry Co., Ltd.**, **Leon Technology Company Limited**; **Megvii Technology Limited**, **Netposa Technologies Limited**, **SZ DJI Technology Co., Ltd., Xiamen Meiya Pico Information Co., Ltd.**, and **Yitu Limited**. As non-SDN CMICCs, US persons are prohibited from purchasing or selling certain publicly traded securities connected with these entities.

State Department Identifies PRC Officials for Undermining Hong Kong Autonomy

On December 20, the State Department submitted an updated report to the US Congress pursuant to the Hong Kong Autonomy Act of 2020. Under the Hong Kong Autonomy Act, the Secretary of State is required to furnish regular updates to Congress that identify foreign persons alleged to have materially contributed to the failure of the PRC to meet its obligations under the Sino-British Joint Declaration or Hong Kong's Basic Law. The December report identified five PRC officials of the Liaison Office of the Central People's Government in Hong Kong (LOCPG), whose actions have allegedly undermined Hong Kong's autonomy. The LOCPG is the PRC's main platform for projecting its influence in Hong Kong. The following five officials were identified: **Chen Dong**, **Lu Xinning**, **Tan Tieniu, He Jing**, and **Yin Zonghua.** As a result of their identification, foreign financial institutions face sanctions for knowingly conducting significant transactions on behalf of the listed officials.

SEC Implements Holding Foreign Companies Accountable Act

On December 3, the US Securities and Exchange Commission adopted a final rule to implement the Holding Foreign Companies Accountable Act. The HFCAA was enacted by Congress on a bipartisan basis and signed into law by former President Trump in December 2020 to allow investors to identify foreign issuers with securities listed on US exchanges and subject their audit reports to the review by the Public Companies Accounting Oversight Board ("PCAOB"). The HFCAA was motivated, in part, by the PCAOB's prior inability to inspect or investigate public accounting firms registered in foreign jurisdictions, including China and Hong Kong. The HFCAA provides for more leverage for the PCAOB to oversee audits of foreign and domestic issuers, as the SEC is authorized to delist companies from US exchanges if they are not subject to PCAOB inspections or investigations for three consecutive years.

At a high level, the final rule creates increased disclosure requirements and allows for the potential delisting of issuers determined to have used registered public accounting firms with branches or offices in a foreign jurisdiction not overseen by the PCAOB, a so-called "Commission-Identified Issuer." Commission-Identified Issuers are then required to provide documentation establishing that the issuer itself is neither owned nor controlled by a governmental entity in the foreign jurisdiction.

If a Commission-Identified Issuer meets the definition of a "foreign issuer," as defined in the Securities and Exchange Act of 1934, more robust disclosures are required in the issuer's annual report filed with the SEC, including:

- information that identifies the PCAOB-identified firm that has prepared the audit report;
- the percentage of the shares of the issuer owned by governmental entities in the foreign jurisdiction where the issuer is registered or otherwise organized;
- whether governmental entities in the foreign jurisdiction with respect to the registered public accounting firm have a "controlling financial interest" with respect to the issuer;

- the names of any Chinese Communist Party ("CCP") officials who are members of the board of directors of the issuer or any affiliated operating entity; and

- whether the articles of incorporation (or any other organizing document) contain any charter of the CCP, including the text of any such charter.

If the SEC finds that an issuer has not submitted documentation to its satisfaction for three consecutive years, the HFCAA requires the SEC to issue an order prohibiting the trading of the company's securities on US stock exchanges and in the US over-the-counter securities markets.

RUSSIA

Developments in Russia this quarter revolved around the now completed, but not yet operational, Nord Stream 2 pipeline. Despite greenlighting the completion of the Nord Stream 2/TurkStream gas pipelines last quarter, the US State Department nonetheless sanctioned a Russian firm and its vessel for their role in the pipeline's construction. As demands for tough NS2-related sanctions grew in Congress, Germany appealed to legislators to temper the calls for harsher measures. President Biden, meanwhile, rallied support from European allies after reports of significant troop build-up at the Russia-Ukraine border, seeking multilateral commitments to leverage NS2 in diplomatic efforts to prevent another Russian invasion.

State Department Sanctions NS2 Developers as Germany Appeals to US Lawmakers

Earlier this year, we reported on the State Department's controversial decision to waive enforcement of sanctions against key figures in the development and completion of the Nord Stream 2 pipeline, including Nord Stream 2 AG (the company overseeing the Nord Stream 2 project) and the company's CEO, Matthias Warnig. Although the waivers remain in place, on November 23, OFAC nevertheless imposed targeted sanctions on a Cyprus-based company, **Transadria**, believed to be a Russian shell company, and a vessel owned by Transadria, **Marlin**, for their involvement in the construction of the Nord Stream 2 gas pipeline.

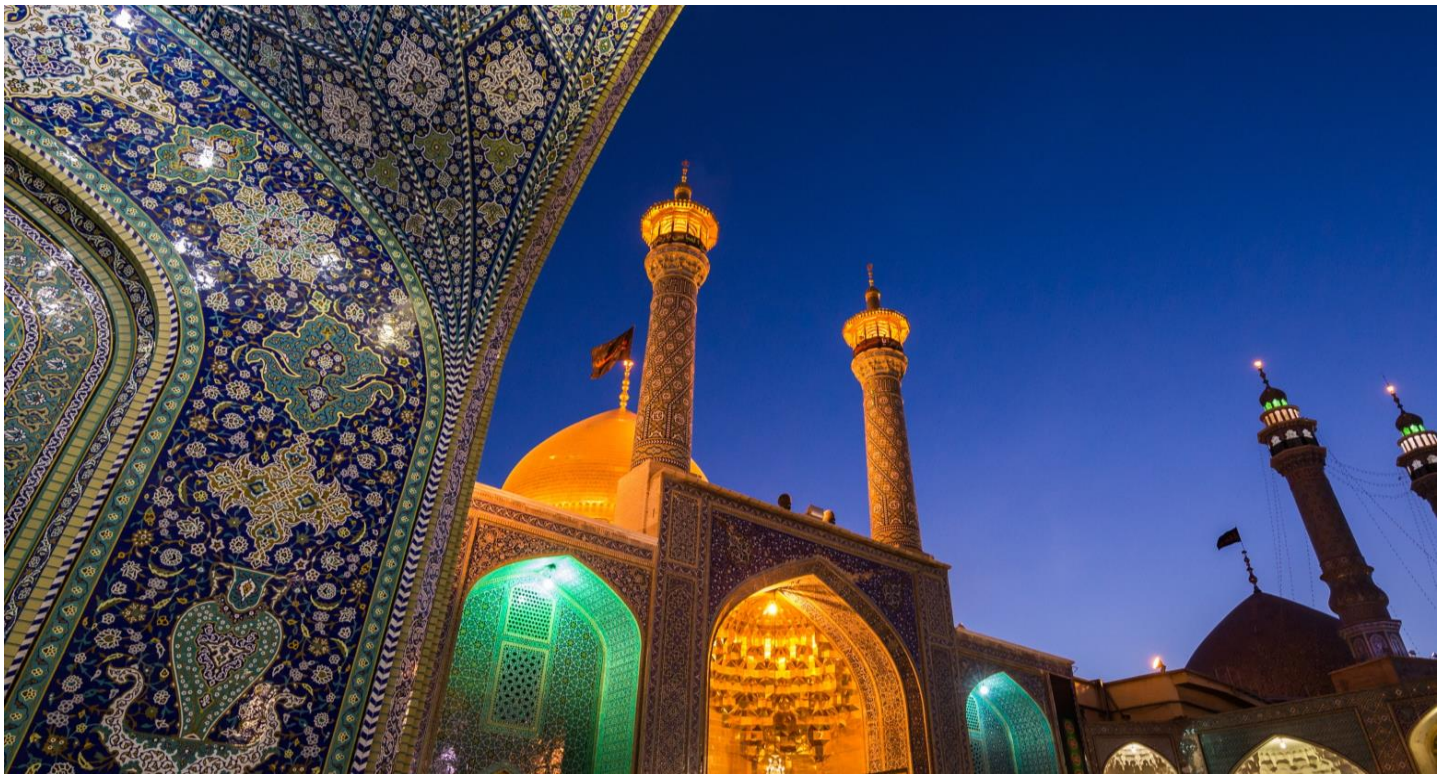
The State Department's decision to waive sanctions in May, which prompted rebukes from members of Congress who threatened to pass legislation to reverse the waiver, has escalated diplomatic tensions between Germany and the US. In November, Germany sought to counter rising demands by US Congressional leaders for the Biden Administration to take a tougher stance on Nord Stream 2 developers. Germany argued that the pipeline does not present a threat to Ukraine and reportedly told legislators that new sanctions would both undermine US commitments to Germany and damage transatlantic unity.

US and EU Unite in Opposition to Russian Aggression Against Ukraine

As Germany sought to temper hostility towards NS2 in Washington, President Biden worked to marshal support from European allies amid reports of troop build-up at the Russia-Ukraine border. The deployment of Russian

military forces sparked fears that Moscow had plans to, once again, invade Ukraine. In 2014, Russia crossed the border and annexed the Crimea Region of Ukraine, resulting in international condemnation, isolation of Russia from the world stage, and a host of sanctions measures designed to punish Russia for what many considered a violation of the principles of international law. A key component of the Biden Administration's campaign is the Nord Stream 2 pipeline, which Washington hopes will serve as a pressure point to deter any Russian aggression. Although construction of the pipeline is complete, it has not yet been certified for operation. As a potential source of significant revenue to Russia, US officials are reportedly seeking assurances from Germany that it will not let the pipeline to become operational if Russia invades Ukraine. As the quarter closed, the US and Russia were engaged in bilateral diplomacy.

IRAN



As negotiations over the revival of the Joint Comprehensive Plan of Action (JCPOA) remain stalled, the US this quarter took only limited action against Iran for its alleged efforts to undermine US election security. Meanwhile, an EU Court issued new guidance on the interpretation of Article 5 of the EU Blocking Regulation.

OFAC Designates Iranian Individuals for Election Interference

On November 18, OFAC designated six Iranian individuals and one entity for attempting to influence the 2020 US Presidential Election pursuant to Executive Order 13848, titled "Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election." OFAC designated Iranian cyber company **Emennet Pasargad** for leading an attempted election influence campaign. According to OFAC, Emennet intruded US state election websites to obtain voter information and accessed the content management accounts of US media outlets to edit and create fraudulent content. Using this information, Emennet then launched an online operation designed to influence American voters through several tactics, including by sending threatening emails to voters and undermining voter confidence through the spread of disinformation regarding election security. OFAC further designated six Iranian nationals alleged to be part of Emmenet's network. These individuals include Emennet's manager **Mohammad Bagher Shirinkar**; Emennet employees **Seyyed Mohammad Hosein Musa Kazemi** and **Sajjad Kashian**; and Emennet directors **Mostafa Sarmadi**, **Seyyed Mehdi Hashemi Toghorljerdi**, and **Hosein Akbari Nodeh**. The Department of Justice additionally unsealed a five-count indictment against **Seyyed Mohammad Hosein Musa Kazemi** and **Sajjad Kashian** concurrent with these designations.

European Court of Justice Issues New Guidance on EU Blocking Regulation

Just as the quarter closed, the Grand Chamber of the Court of Justice of the European Union ("CJEU"), EU's top court, found that EU operators are permitted to end contracts with Iranian companies subject to US sanctions if honoring their contractual obligations would cause "disproportionate economic loss" to the company. The opinion, issued upon a referral from a lower court sitting in Hamburg, Germany, is the latest in the long-running case *Bank Melli Iran v. Telekom Deutschland GmbH*. The dispute concerns Telekom Deutschland GmbH's (a subsidiary of Deutsche Telekom) termination of its contractual relationship with Bank Melli Iran when Bank Melli

again came under US sanctions in 2018. Bank Melli Iran challenged the termination and argued that Telekom Deutschland violated the EU Blocking Statute. The Blocking Statute provides that no EU company shall take actions based on the threat of extraterritorial sanctions. It was enacted to protect European companies from the risk of US sanctions, and to preserve the JCPOA framework after President Trump withdrew the US from the multilateral accord. In plain terms, the Blocking Statute provides that no EU company shall take actions based on the threat of extraterritorial sanctions.

The Grand Chamber's opinion provides important clarifications for national courts to consider when entertaining civil proceedings alleging violations of the Blocking Statute. The Grand Chamber opined that:

- The prohibitions in Article 5 of the Blocking Statute apply even where compliance with US sanctions has not been ordered by a US administrative or judicial authority.

- While the Blocking Statute does not necessarily require EU operators to give reasons for terminating a contract with sanctioned persons, when challenged in a civil proceeding in EU courts, the operator nevertheless bears the burden of proof to establish that termination did not seek to comply with US sanctions.

- In assessing whether an EU operator can, within the terms of the Blocking Statute, terminate a contract based on a desire to comply with US sanctions, the Grand Chamber opined that national courts must consider the terms of the Blocking Statute but also give weight to the right of an operator to freely conduct its business. In applying principles of proportionality, the Grand Chamber instructed lower courts to balance the need to give effect to EU statutory objectives against the potential for "disproportionate economic consequences" that might arise from the application of US sanctions if an operator were unable to terminate its contract with a sanctioned person.

Once again, the opinion provides only interpretive guidance and national courts are left to grapple with the weighty political and economic considerations presented in challenging commercial circumstances. Nevertheless, the opinion implies that EU operators seeking to terminate contracts for reasons unrelated to US sanctions should properly document those reasons to meet its burden of proof. If, however, US sanctions are a reason for termination, an EU operator would be well advised to document the consequences, political and financial, that the imposition of US sanctions could have on its business.

US TARGETS CYBER-OPERATORS AND SPYWARE DEVELOPERS

As we reported last quarter, the Biden Administration is taking a "whole of government approach" to combat the use of ransomware, including by targeting malign cyber actors and virtual currency exchanges that facilitate their financial transactions. After releasing a government-wide ransomware advisory and advice for virtual currency exchanges, OFAC on November 8 designated Ukrainian national **Yaroslav Vasinskyi** and Russian national **Yevgeniy Polyanin** for their roles in the Sodinokibi/REvil ransomware attacks against the United States. Vasinskyi reportedly was involved in ransomware attacks against at least nine US companies, including the July 2021 ransomware attack against IT management company Kaseya. Polyanin reportedly conducted ransomware attacks against US government entities and companies. Together, they have received over $200 million in cryptocurrency ransom payments.

Shortly thereafter, on November 9, the US Treasury Department announced a set of actions focused on virtual currency exchanges used to launder the proceeds of ransomware attacks. Pursuant to Executive Order 13694, which targets those responsible for or complicit in malicious cyber-enabled activities, OFAC designated virtual currency exchange **Chatex**, for facilitating transactions on behalf of ransomware actors across multiple countries and for multiple ransomware variants. According to OFAC, Chatex has ties to SUEX OTC, S.R.O., which was sanctioned on September 21, 2021. OFAC also designated **IZIBITS OU**, **Chatextech SIA**, and **Hightrade Finance Ltd** for providing material support and assistance to Chatex.

Meanwhile, on the heels of the well-publicized Russian-state attack against SolarWinds earlier this year, Microsoft Corporate Vice President Tom Burt reported in October that Russia-linked cyber actors had infiltrated Microsoft systems in an attack described as "very large" and "ongoing." Microsoft alerted 609 customers about 22,868 attacks by Nobelium, a malign cyber actor, between July 1 and October 19, with a success rate in the low single digits. Microsoft reported that the number of attacks it received in the last three months was greater than the number of attacks it received in the past three years combined, suggesting that Russian cyber-spies have not felt the impact of recent US sanctions. Earlier this year, President Biden announced sanctions on Russian financial institutions and technology companies following the alleged Russian-state attack on US company, SolarWinds.

In related developments, the Department of Commerce sought to curb the export of US-origin goods that support the supply of spyware and cyber-enabled tools to foreign governments for purposes of espionage. In November, the Bureau of Industry and Security added a number of foreign companies to its Entity List for their alleged sale of these goods to foreign governments. Among those added to the Entity List was **NSO Group**, an Israeli spyware company that makes the phone-hacking technology Pegasus. NSO Group reportedly sold Pegasus to foreign governments who then used it to target government officials, journalists, business people, activists, academics, and embassy workers. In a statement, BIS called the effort a threat to the "rules-based international order." BIS also added Israeli company **Candiru**, Russian company **Positive Technologies**, and Singaporean company **Computer Security Initiative Consultancy PTE, LTD** to the Entity List for supplying spyware and other cyber tools to foreign governments. As a result of their addition to the Entity List, each company will be prohibited from receiving US-origin goods, software, and technology absent an export license granted by the Department of Commerce.

OFAC TARGETS CORRUPT ACTORS AND HUMAN RIGHTS VIOLATORS AROUND THE WORLD

On November 10, two Cambodian government officials were designated pursuant to E.O. 13818, which builds upon and implements the Global Magnitsky Human Rights Accountability Act and targets perpetrators of serious human rights abuse and corruption around the world. In this action, OFAC designated **Chau Phirun** and **Tea Vinh**, both high-ranking officials within the Cambodian Ministry of National Defense, for significant corruption in skimming personal profits from construction projects of military facilities. According to OFAC, Chau conspired to profit in 2020-2021 from activities related to the construction of the Ream Naval Base, while both Chau and Tea inflated the cost of the naval base facilities to skim profits. Concurrently, the State Department imposed visa restrictions against Chau, Tea, and their immediate family members.

In the leadup to the US-organized Summit for Democracy, OFAC announced a host of actions designed to punish corrupt actors and perpetrators of serious human rights abuses. In the first such announcement, OFAC designated **Alain Mukonda** and twelve entities under his control for allegedly providing support to sanctioned billionaire Dan Gertler in the Democratic Republic of the Congo. Gertler was previously designated upon allegations that he manipulated the DRC political system for economic gain, including by amassing hundreds of millions of dollars from corrupt mining and oil deals in the DRC. In what OFAC called a "financial lifeline," Gertler now relies on the support of those like Mukonda, who opened bank accounts and made millions of dollars' worth of deposits to Gertler's benefit. Additionally, Mukonda reportedly domiciled several of Gertler's companies from Gibraltar and the British Virgin Islands to the DRC.

On December 7, OFAC designated fifteen individuals for committing serious human rights abuses against civilians, political opponents, and peaceful protesters that have the effect of undermining democracy. The designations included government officials in three different countries. OFAC designated Major General **Abel Kandiho**, the commander of the Ugandan Chieftaincy of Military Intelligence (CMI), for his involvement in the arrest, detention, and gross physical abuses of persons in Uganda based on their nationality and political views. Among those sanctioned for suppression of peaceful protesters and repression in Iran were the **Special Units of Iran's Law Enforcement Forces**. According to OFAC, the LEF Special Units work within Iran's security apparatus

and are dedicated to crowd control and the violent suppression of peaceful protests. In one notable example from November 2019, the LEF Special Units and a subunit known as **Iran's Counter-Terror Special Forces**, fired upon and killed unarmed protesters with automatic weapons. OFAC also designated a host of individuals connected to the LEF Special Units and other units of Iran's security apparatus. Finally, OFAC designated two Syrian Air Force officials, **Tawfiq Muhammad Khadour** and **Muhammad Youssef Al-Hasouri**, alleged to have carried out airstrikes during which lethal chemical weapons were dropped on Syrian civilians. A full listing of those designated in these actions can be found at this link.

On December 8, OFAC targeted corrupt actors linked to transnational organized crime networks across the world. In this action, sixteen individuals and twenty-four entities were designated pursuant to E.O. 13818. Noting that "organized crime and corruption are often linked," OFAC sanctioned sixteen individuals and twenty-four entities across a host of countries, including the Balkan countries and in El Salvador. Chief among those designated for illicit activity in Kosovo was **Zvonko Veselinovic**, the leader of Zvonko Veselinovic Organized Crime Group. According to OFAC, the OGC traffics in goods, money, narcotics and weapons after bribing Kosovar and Serbian security officials. Veselinovic and his associates also leverage their support to political candidates in exchange for promises not to interfere with their illegal schemes. In addition to Veselinovic, OFAC designated other OGC members and a host of entities under their control.

OFAC designated two El Salvadorian government officials who allegedly facilitated a series of covert meetings between known gang members and gang leaders incarcerated in prison. In one such scheme, **Osiris Luna Meza (Luna)** and **Carlos Amilcar Marroquin Chica** negotiated with gang leaders to develop a truce under which MS-13 and Barrio 18 gangs would curb the number of gang-related homicides in exchange for money and the promise of political support to El Salvadoran President Nayib Bukele's political party.

Coinciding with International Corruption Day, on December 9, OFAC designated a host of corrupt actors across the world, some of whom are alleged to have exploited Covid-19 pandemic relief for personal gain. OFAC designated **Martha Carolina Recinos De Bernal**, a Salvadoran government official for corrupt schemes involving pandemic-related goods and supplies. Specifically, Recinos allegedly received kickbacks for awarding inflated government contracts to procure pandemic-related goods like masks and hospital gowns to companies that had no apparent ties to the healthcare sector. In another scheme, Recinos diverted critical medical supplies to specific districts to garner support for candidates in President Bukele's political party. OFAC also designated **Manuel Victor Martinez Olivet** was sanctioned for awarding government contracts in Guatemala to family members without going through the public bidding process. Meanwhile, OFAC designated the former Deputy Head of the Ukrainian Presidential Administration and notorious "court fixer," **Andriy Portnov**, who used his influence to place loyal officials in senior judiciary positions and then purchase judicial decisions. In total, OFAC designated fifteen individuals and entities across several countries in Europe, Africa, and Central America.

COUNTERTERRORISM DESIGNATIONS

On October 26, OFAC, in conjunction with an action by the United Nations Security Council, sanctioned Libyan national **Osama Al Kuni Ibrahim** for human rights abuses against migrants in Libya. OFAC reports Al Kuni is the de facto manager of the Al Nasr Detention Center in Zawiyah, Libya, where migrants face extreme abuse and exploitation including sexual violence, beatings, starvation, and, in some cases, death. Al Kuni is sanctioned under E.O. 13726 for his involvement in violent attacks targeting civilians.

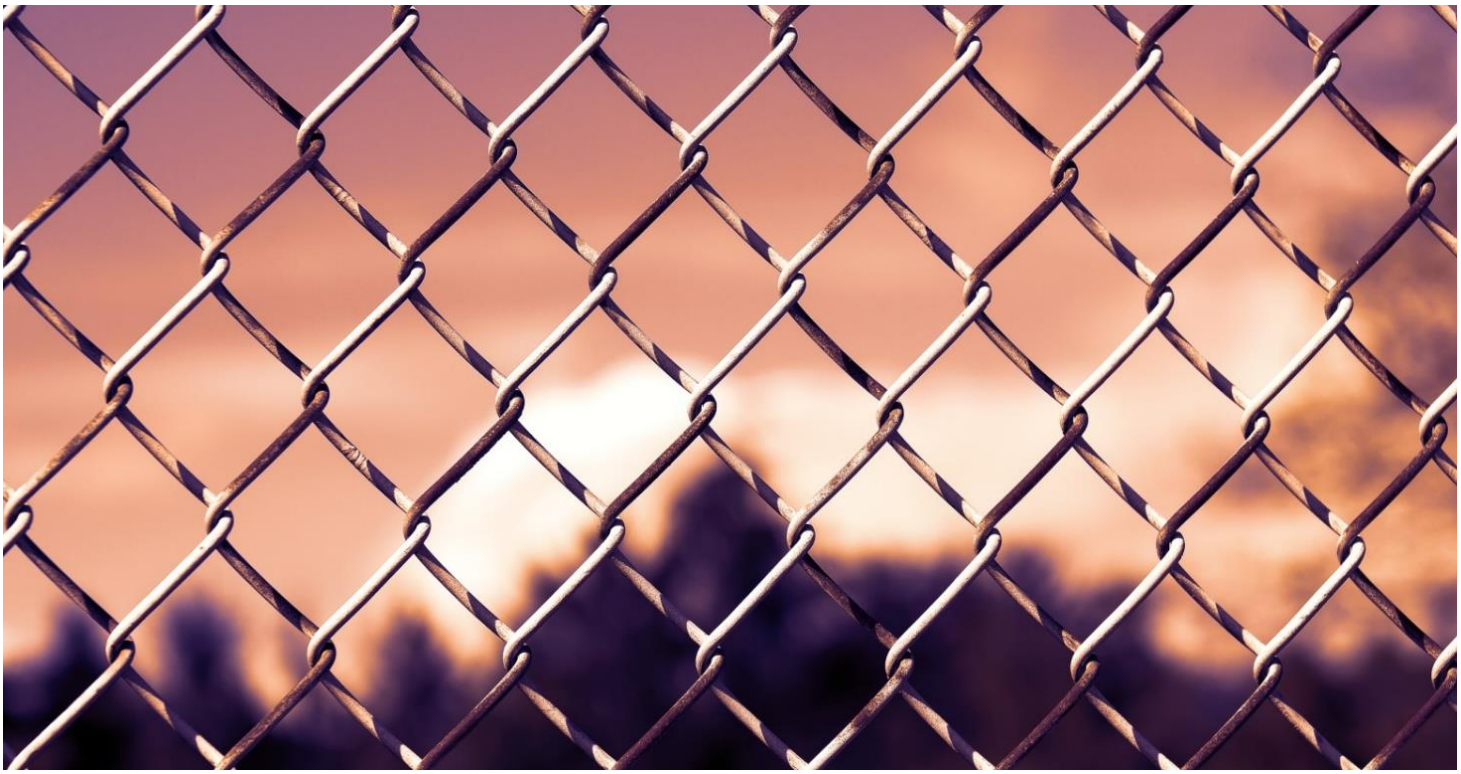
On October 29, OFAC designated three Iranian individuals and three entities affiliated with the unmanned aerial vehicle ("UAV") programs of Iran's Islamic Revolutionary Guard Corps and the IRGC-Qods Force. The actions were taken pursuant to E.O. 13223, addressing counterterrorism, and E.O. 13382, which targets proliferators of weapons of mass destruction. OFAC designated IRGC Brigadier General **Saeed Aghajani**, who oversees the IRGC ASF UAV Command that orchestrated the July 29, 2021 attack on a commercial shipping vessel off the coast of Oman. OFAC also designated IRGC Brigadier General **Abdollah Mehrabi** for having procured UAV engines for his company, **Oje Parvaz Mado Nafar Company**. The company, and its managing director **Yousef Aboutalebi**, were also designated for their roles in supporting weapons development for the IRGC and the Iran Qods Aviation Industries and Aircraft Manufacturing Industries, both already subject to sanctions. Finally, OFAC designated **Kimia Part Sivan Company**, an Iranian entity that has worked with Iran's Qods Force to improve its UAV program and procures UAV components for the IRGC. OFAC further designated **Mohammad Ebrahim Zargar Tehrani** for assisting the company in sourcing these components.

On November 22, OFAC designated a financial facilitator for ISIS-Khorasan Province ("ISIS-K"), a branch of the Islamic State terrorist group active in Afghanistan. Operating from Turkey, Afghanistan, and the United Arab Emirates, **Ismatullah Khalozai** has reportedly run numerous businesses, including a Turkish hawala business and a UAE-based luxury items resale business, in support of ISIS-K. Khalozai has also reportedly carried out human smuggling operations for ISIS-K. OFAC designated Khalozai for providing material support to ISIS-K. On the same day, the U.S. Department of State designated **Sanaullah Ghafari**, **Sultan Aziz Azam**, and **Maulawi Rajab** as Specially Designated Global Terrorists ("SDGT") for operating as leaders of ISIS-K.

On November 30, the State Department revoked the designations of the **Revolutionary Armed Forces of Colombia** ("FARC") as a foreign terrorist organization and as an SDGT but designated the **Revolutionary Armed Forces of Colombia – People's Army** ("FARC-EP") and **Segunda Marquetalia** as foreign terrorist organizations and SDGTs. The State Department also designated numerous high-level individual members of those organizations: **Luciano Marin Arango**, the founder and leader of Segunda Marquetalia, **Hernan Dario Velasquez Saldarriaga**, a senior commander in Segunda Marquetalia, **Henry Castellanos Garzon**, a senior leader in Segunda Marquetalia, **Nestor Gregorio Vera Fernandez**, the commander and leader of FARC-EP, **Miguel Santanilla Botache**, a commander in FARC-EP, and **Euclides Espana Caicedo**, the most senior commander of multiple units of the FARC-EP.

On December 22, OFAC designated three individuals and two entities operating in Brazil for providing material support to al-Qa'ida. OFAC designated an early member of an al-Qa'ida network in Brazil, **Haytham Ahmad Shukri Ahmad Al-Magrhabi** (Al-Magrhabi), who reported to and was the key contact for Ahmed Mohammed Hamed Ali, al al-Qa'ida operative designated as an SDGT on October 12, 2001. OFAC further designated two individuals, **Mohamed Sherif Mohamed Awadd** and **Ahmad Al-Khatib**, and the furniture businesses with which they are affiliated, **Home Elegance Comercio de Moveis EIRELI** and **Enterprise Comercio de Moveis e Intermediacao de Negocios EIRELI**, for providing material support to designated al-Qa'ida operatives.

OFAC TARGETS NARCOTICS TRAFFICKERS & CRIMINAL ORGANIZATIONS



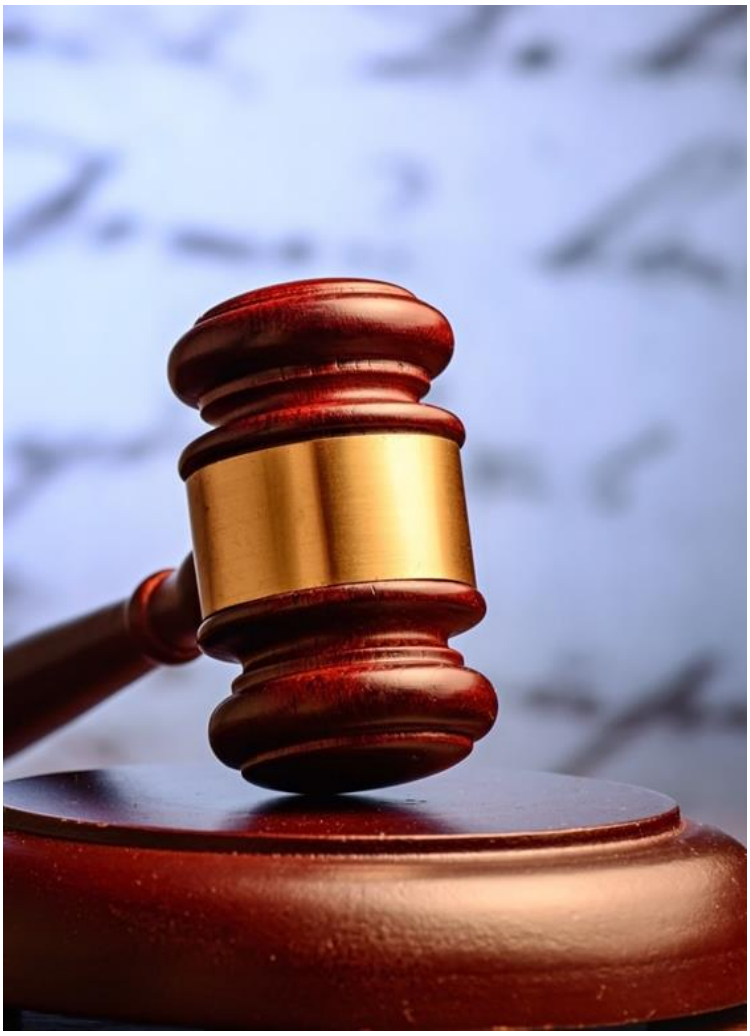
On October 6, OFAC designated four Mexican nationals alleged to be members of the **Cartel de Jalisco Nueva Generacion ("CJNG")** pursuant to the Kingpin Act. According to OFAC, **Aldrin Miguel Jarquin Jarquin**, **Jose Jesus Jarquin Jarquin**, **Cesar Enrique Diaz De Leon Sauceda**, and **Fernando Zagal Anton** are responsible for trafficking fentanyl and other deadly drugs through the port of Manzanillo in Colima, Mexico. Manzanillo port, located on the Pacific coast, is a gateway for Colombian cocaine and chemicals used to synthesize fentanyl. The four individuals are designated for providing support to CJNG and have links to previously designated individuals, including the son-in-law of CJNG leader Ruben Oseguera Cervantes. These designations are the fifteenth OFAC action against CJNG for its role in international narcotics trafficking.

On December 15, President Biden issued two executive orders aimed at combatting transnational criminal organizations trafficking drugs in the United States. The first executive order formally establishes a US Council on Transnational Organized Crime, which includes Cabinet-level representation from the Departments of Justice, Homeland Security, Treasury, State, Defense, and the Office of the Director of National Intelligence. The second executive order, entitled "Imposing Sanctions on Foreign Persons Involved in the Global Illicit Drug Trade," enables OFAC to designate individuals engaged in drug trafficking activities without first finding a link to a specific kingpin or cartel.

In conjunction with the executive orders, OFAC designated ten individuals and fifteen entities in Brazil, China, Colombia, and Mexico for their involvement in international drug trafficking and highlighted a few of the newly designated individuals and entities. Related to Brazil, OFAC designated **Primeiro Comando Da Capital**, which OFAC calls the most powerful organized crime group in Brazil and among the most powerful in the world. OFAC designated Chinese national **Chuen Fat Yip** for trafficking fentanyl, anabolic steroids, and synthetic drugs to the US and selling compounds and chemicals to similarly designated Chinese entity **Wuhan Yuancheng Gongchuang Technology Co. Ltd**. OFAC also designated **Shanghai Fast-Fine Chemicals Co., Ltd.**, **Hebei Huanhao Biotechnology Co., Ltd.**, and **Hebei Atun Trading Co., Ltd**. OFAC designated two splinter groups of the Beltran Leyva Organization, **Los Rojos DTO** and **Guerreros Unidos**, operating in Mexico. Finally, OFAC

designated **Clan del Golfo**, a well-armed drug trafficking organization operating in Colombia with links to cartels in Costa Rica, Honduras, Panama, Guatemala, and Mexico, and its leader **Dairo Antonio Usuga David**, previously designated under the Kingpin Act in 2010.

ENFORCEMENT ACTIONS



On November 9, OFAC announced that it had issued a Finding of Violation to Dubai-based **Mashreqbank psc** for 1,760 apparent violations of the Sudanese Sanctions Regulations arising from the processing of payments through US financial institutions related to US dollar transfers from Sudanese bank accounts. Specifically, between January 4, 2005 and February 9, 2009, Mashreqbank's London branch processed 1,760 outgoing payments through US financial institutions from accounts of Sudanese banks held outside of the US. According to OFAC, Mashreqbank did not populate the optional field in the SWIFT payment messages that would identify the originating Sudanese institution, which rendered the US correspondent bank accounts of Mashreqbank unable to detect the involvement of Sudanese accounts and interdict the payments. The failure to populate this field was contrary to then-applicable SWIFT protocols, general banking practice, and Mashreqbank's own standard procedures. By processing these payments, Mashreqbank caused US persons to export services from the US to Sudan in violation of US sanctions.

Although OFAC found Mashreqbank to have acted recklessly and to have weak internal controls, OFAC determined a Finding of Violation ("FOV") was sufficient in lieu of a civil monetary penalty, in part because of Mashreqbank's willingness to enter into a retroactive statute of limitations waiver agreement without which the prosecution of these violations would have been time-barred. The FOV was part of a global settlement between Mashreqbank, the New York State Department of Financial Services, and the Federal Reserve Board of Governors.

On December 8, 2021, OFAC announced that it had reached a settlement with an individual **US person** to settle that person's potential civil liability arising under US sanctions against Iran. Between February 2016 and March 2016, the US Person accepted payment on behalf of an Iran-based company that sold Iranian-origin cement clinker to a separate company for use abroad. According to OFAC, the US Person arranged for and received four payments, totaling $133,860 into his personal bank account in the United States in connection with the sale of cement clinker from an Iranian company. The US Person coordinated the sale of the clinker with the help of a family member who worked at the Iranian company and served as an intermediary between the Iranian company and the third-country purchaser. OFAC further alleged that the US Person knew or had reason to know that the conduct was prohibited. For example, the US Person previously applied for, but was denied, a license from OFAC to authorize transactions with Iran, and was informed by the Iranian company of the complications involved in accepting US dollar payments. In determining the $133,860 settlement amount, OFAC noted that the conduct was not voluntarily disclosed and that it constituted an egregious case.

On December 23, **TD Bank, N.A.** agreed to pay a $115,005 penalty to settle two matters involving apparent violations of the North Korea Sanctions Regulations and the Foreign Narcotics Kingpin Sanctions Regulations. In the first matter, OFAC alleged that the bank processed 1,479 transactions totaling $382,685.38 between December 2016 and August 2018 and maintained nine accounts on behalf of employees of the North Korean mission to the United Nations without a license from OFAC. US sanctions against North Korea prohibit US

financial institutions from opening and operating accounts for employees of the North Korean mission. The software used to screen customers at account opening allegedly relied heavily on a list of politically exposed persons and did not include the names of government employees of sanctioned countries.

In the second matter, the bank maintained two accounts over a four-year period for Esperanza Caridad Maradiaga Lopez, who was designated as an SDN in 2013. In 2016, Lopez opened two accounts at a branch in Miami, Florida. A bank employee allegedly dismissed an alert that flagged for the bank's compliance department the possible match with the SDN List because there was no full match on the person's name, date of birth, and geographical location. OFAC said that four additional alerts for Ms. Lopez were generated, all of which were manually dismissed by bank employees, though her accounts were finally closed after a reviewer determined the alert to be a true hit. The asserted compliance failures, including human errors and a breakdown in official compliance procedures, led to 145 apparent violations of the Foreign Narcotics Kingpin Sanctions Regulations. OFAC noted that the apparent violations in both matters were voluntarily self-disclosed and were non-egregious.

ABU DHABI
AUSTIN
BEIJING
BRUSSELS
DALLAS
DUBAI
FRANKFURT
HONG KONG
HOUSTON
LONDON
MENLO PARK
MILAN
MUNICH
NEW YORK
PARIS
RIYADH*
ROME
SAN FRANCISCO
SÃO PAULO
SHANGHAI
SINGAPORE
TOKYO
TORONTO
WASHINGTON, DC

Shearman & Sterling has long advised financial institutions and commercial businesses on the most complex sanctions issues. If you have any questions, please feel free to contact one of our partners or counsel.

Authors & Contributors

Philip Urofsky

Danforth Newcomb

Stephen Fishbein

Brian G. Burke

Christopher L. LaVigne

Barnabas Reynolds

Mark D. Lanpher

Paula Howell Anderson

Adam B. Schwartz

Katherine J. Stoller

Associate Contributors

Jacob Fields

Cole Pritchett

Blair Campion

Related Services

Sanctions, Litigation, Anti-Corruption & Foreign Corrupt Practices Act (FCPA)

SHEARMAN & STERLING