

# 2020 Mid-Year Sanctions and Export Controls Update

Client Alert | August 4, 2020

---

The ongoing coronavirus has caused governments and populations to rethink how to conduct social interactions and in turn how to conduct business on a global scale. Despite the ongoing global public health crisis, the United States Government's efforts to use its economic leverage to conduct foreign policy continues unabated. Indeed, throughout the first half of 2020, the United States continued to tighten the screws on Iran and Venezuela and has not shied away from using its economic arsenal in its escalating trade war with China.

As the global pandemic has deepened, there have been calls from some quarters, including from UN Secretary General [António Guterres](#) and UN High Commissioner for Human Rights [Michelle Bachelet](#), for a temporary easing of sanctions—on humanitarian and public health grounds—against countries especially vulnerable to the spread of COVID-19, including Iran and Venezuela. U.S. officials have so far declined that invitation, [citing](#) the broad humanitarian exceptions already incorporated into U.S. sanctions measures. Underscoring the point, the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") in April 2020 issued a [fact sheet](#) compiling all of the existing authorizations and exemptions for humanitarian trade and other assistance with respect to each comprehensively sanctioned jurisdiction, including Iran. This suggests that, for now at least, OFAC views its existing exemptions and authorizations as sufficient to meet the current public health emergency and has no intention or appetite for otherwise easing sanctions.

The pandemic has only further highlighted U.S.-China tensions and, unsurprisingly, the United States has continued to use sanctions and export controls not only to apply pressure in the escalating trade war but in response to China's human rights abuses in Hong Kong and against the country's Uyghur minority.

More broadly, the U.S. administration and OFAC have taken several measures to remind the world that compliance with economic sanctions remains of paramount importance despite the global upheaval. Even in the midst of the pandemic-induced chaos, OFAC still found time to issue an entirely [new sanctions program](#) addressing the humanitarian situation in Mali and has continued to take additional measures targeting Syria and North Korea. OFAC and BIS designations have continued apace, and the State Department has even gotten into the game by designating an increasing number of individuals as "Corrupt Actors" and "Human Rights Violators." Taking a warning shot across the bow of the shipping industry, in May 2020, OFAC [issued](#) the latest in a series of industry advisories addressing deceptive practices in global maritime transportation, building upon previously published guidance relating to North Korea's, Syria's, and Iran's illicit shipping practices. The advisory stresses that 90 percent of global trade involves maritime transportation, and that, even during a massive international public health crisis, participants must remain vigilant.

## I. Major U.S. Program Developments

### Related People

[Judith Alison Lee](#)

[Adam M. Smith](#)

[Christopher T. Timura](#)

[Scott R. Toussaint](#)

[Samantha Sewall](#)

[Audi K. Syarief](#)

## A. Iran

During the first half of 2020, the United States continued to increase sanctions pressure on the regime in Tehran while also seeking to enable the flow of humanitarian goods and services to the Iranian people to alleviate the suffering due to COVID-19. Notably, amid a spike in tensions between Washington and Tehran following the January 2020 killing of Iranian General Qassem Soleimani in a U.S. airstrike, the Trump Administration imposed secondary sanctions on some of the few remaining sectors of the Iranian economy not already subject to U.S. restrictive measures. Meanwhile, as Iran grappled with one of the first severe outbreaks of COVID-19, OFAC leveraged its existing authorities to facilitate the provision of aid to the Iranian people, including by opening a new Swiss channel for humanitarian trade and authorizing certain transactions to flow through Iran's central bank.

On January 10, 2020, President Trump issued [Executive Order 13902](#), which authorizes OFAC to designate entities operating in the construction, mining, manufacturing, or textiles sectors of the Iranian economy, as well as *any other sector* of the Iranian economy targeted by the U.S. Secretary of the Treasury. The order also authorizes the imposition of secondary sanctions against any non-U.S. person or company that knowingly engages in a significant transaction involving one of those targeted sectors. Following the expiration of a [90-day wind-down period](#) on June 5, 2020, OFAC published [guidance](#) indicating how the agency expects to define those four sectors, as well as what types of dealings in goods and services are potentially sanctionable. For example, in light of the COVID-19 pandemic, OFAC [clarified](#) that the new manufacturing sanctions do *not* target persons or companies in Iran manufacturing medicines, medical devices, or products used for sanitation, hygiene, medical care, medical safety, and manufacturing safety (e.g., soap, hand sanitizer, ventilators, respirators, personal hygiene products, diapers, infant and childcare items, personal protective equipment, and manufacturing safety systems), solely for use within Iran and not for export abroad.

Additionally, consistent with longstanding U.S. policy in favor of legitimate humanitarian trade with sanctioned jurisdictions, the United States during the past six months also implemented several measures designed to facilitate Iran's response to the coronavirus pandemic.

OFAC, building on a [framework](#) announced in October 2019 under which foreign governments and foreign financial institutions may establish approved payment mechanisms for humanitarian exports to Iran, in February 2020 announced that the first such payment channel has become operational. Developed in cooperation with the Swiss government, the [Swiss Humanitarian Trade Arrangement](#) is a voluntary mechanism under which OFAC will provide written confirmation, or "comfort letters," to persons domiciled in Switzerland (including entities owned or controlled by U.S. persons), affirming that sales to Iran of food, agricultural commodities, medicine, and medical devices are not exposed to U.S. sanctions. To obtain these comfort letters, exporters must submit to stringent due diligence and reporting requirements to ensure that humanitarian exports are not improperly diverted to sanctioned parties. Given those exacting requirements, however, the number of transactions processed through the new Swiss payment channel so far remains relatively small.

In February 2020, OFAC issued Iran [General License 8](#), which authorizes certain humanitarian transactions involving the Central Bank of Iran ("CBI"). Entities designated under OFAC's [counterterrorism authorities](#), including as of last year the CBI, are not only subject to the broad sanctions restrictions typically imposed on SDNs, but also may not participate in humanitarian trade with Iran—a category of activity generally exempt from sanctions restrictions. General License 8 therefore creates an exception under which both [U.S. persons and non-U.S. persons](#) are authorized to engage in certain transactions with the CBI involving sales to Iran of food, agricultural commodities, medicine, and medical devices. Notably, that exception is [specific to the CBI](#) and does *not* extend to transactions

involving any other Iranian financial institution sanctioned under a U.S. counterterrorism authority, such as [Executive Order 13224](#).

Moreover, as part of its “maximum pressure” campaign, the Trump administration has continued to tighten sanctions on Iranian transactions and activities that do not raise humanitarian concerns. In May 2020, the U.S. Department of State [announced](#) that, subject to a [60-day wind-down period](#) that expires on July 27, 2020, the United States is ending sanctions waivers that have allowed non-U.S. persons to engage in certain activities involving Iran’s civil nuclear program. The United States in May and June also designated a steady stream of Iranian targets, including [military front companies](#), [senior law enforcement officials](#), [ship captains](#), and [metals producers](#). With a U.S. presidential election looming in November 2020, such Iran-related designations will likely continue apace throughout the months ahead.

## B. Venezuela

Despite presiding over a collapsing economy, a deepening public health crisis, and the exodus of several million of its citizens, the regime of President Nicolás Maduro presently controls nearly all levers of power within Venezuela, including the country’s courts and armed forces. Expanding on earlier sanctions measures, the Trump administration during the first half of 2020 deployed an array of tools to deny the Maduro regime the resources and support necessary to sustain its hold on power—from indicting several of Venezuela’s top leaders to aggressively targeting virtually all dealings with Venezuela’s crucial oil sector.

In March 2020, the U.S. Department of Justice [announced](#) criminal indictments against President Maduro and 14 other high-level officials, including Venezuela’s chief justice and defense minister. The indictments allege a wide range of criminal conduct by Venezuela’s senior leadership, including overseeing a cartel that imported significant quantities of cocaine into the United States, corruption, money laundering, and sanctions evasion. While not formally a sanctions action, the announcement was notable because the United States, as a matter of policy, does not charge [sitting heads of state](#)—a restriction that was determined not to apply because the United States and nearly 60 other countries do not [recognize](#) Maduro as Venezuela’s rightful leader. In addition to constricting the officials’ ability to travel overseas for fear of being arrested and extradited, the indictments also potentially dim the prospects for a negotiated settlement to Venezuela’s political crisis if, upon ceding power, President Maduro and his top lieutenants face the prospect of being jailed in New York.

In addition to leveraging the criminal justice system, the Trump administration over the past six months repeatedly sanctioned (or threatened to sanction) non-U.S. persons for playing even an indirect role in bringing Venezuelan oil to market.

In February and March 2020, OFAC [designated](#) two [subsidiaries](#) of the Russian state-controlled oil giant Rosneft for brokering the sale and transport of Venezuelan crude—prompting Rosneft to [announce](#) shortly afterward that it will cease all operations in Venezuela and sell its Venezuelan assets to an unnamed company wholly owned by the Kremlin. However, this shift does not necessarily mean that Russia is abandoning its alliance with the Maduro regime or even its involvement in Venezuela’s oil industry. Rather, the transaction appears designed to protect Rosneft—the centerpiece of Russia’s oil sector—from the imposition of deeper U.S. sanctions by walling off all Venezuela-related dealings inside a special purpose entity that is perhaps less vulnerable to U.S. sanctions pressure than a large, publicly traded company.

In April 2020, OFAC further restricted dealings with Venezuela’s oil sector by narrowing one of the few remaining authorizations for U.S. companies to engage in dealings with the state-owned oil company Petróleos de Venezuela, S.A. (“PdVSA”). Since the United States imposed sanctions on PdVSA in January 2019, OFAC has issued, and repeatedly

extended, a general license authorizing five named U.S. oil and oil field services companies to engage in all transactions and activities ordinarily incident and necessary to operations in Venezuela involving PdVSA and its various subsidiaries. This authorization was designed to enable specific *empresas mixtas*, which are joint ventures between large multinational energy companies and PdVSA, to continue operating.

The latest version of that [license](#), issued on April 21, 2020, is more limited in scope—authorizing, until December 1, 2020, just certain “essential” activities involving those five companies’ joint ventures, including activities ordinarily incident and necessary to protecting the safety of personnel, preserving assets, and participating in shareholder and board meetings. OFAC now expressly excludes from the authorization a number of key activities, including (1) drilling, lifting, processing, purchasing, selling, or transporting Venezuelan-origin petroleum and petroleum products; (2) repairs or improvements to Venezuelan energy infrastructure; and (3) the payment of dividends to PdVSA entities. Moreover, the license for the first time provides for—but does not require—the wind down of the five companies’ dealings with PdVSA. By effectively prohibiting U.S. firms from extracting and selling Venezuelan-origin petroleum, this policy shift calls into question the continuing viability of the *empresas mixtas* more generally—at least after December 1, 2020. Though the general license could be renewed once more, if the five U.S. companies named in the license—and their non-U.S. peers, including a number of leading European energy firms with similar ventures—were ultimately to depart Venezuela, the United States stands to lose a foothold in an OPEC member state with enormous proven oil reserves.

Finally, reflecting the breadth of the Trump administration’s efforts to disrupt the Venezuela oil trade, OFAC in June 2020 repeatedly designated [shipping companies](#) and [tankers](#) for lifting Venezuelan crude. While these companies and their vessels were eventually [de-listed](#) following enhancements to their sanctions compliance programs and pledges to cease involvement with Venezuela’s oil sector for so long as the Maduro regime remains in power, these actions—coupled with [reports](#) of imminent plans by OFAC to designate dozens more vessels—have caused maritime companies to re-evaluate their exposure to Venezuela. Indeed, ship owners, managers and operators, flag registries, port operators, insurance companies, and financial institutions are now effectively on notice that, absent authorization from OFAC, any involvement in transporting Venezuelan oil is now highly risky.

## C. Syria

As the almost decade-old conflict in Syria persists, the U.S. Government has continued to use economic sanctions as a means to pressure the Assad regime as well as other actors in the region who continue to commit human rights abuses against the Syrian civilian population. On June 17, 2020 the [Caesar Syria Civilian Protection Act of 2019](#) (“Caesar Act” or the “Act”) went into effect (180 days since its signing by President Trump as part of the 2020 National Defense Authorization Act). The Caesar Act, named after the Syrian defector known as “Caesar” who smuggled out photographs of torture occurring under the Assad regime, was implemented by Congress to, [in the words of Secretary Pompeo](#), “promote accountability for brutal acts against the Syrian people by the Assad regime and its foreign enablers.” The Act requires the President, at the 180-day mark, to take certain actions, including with respect to the Act’s sanctions provisions. The provisions strengthen secondary sanctions with respect to Syria by requiring the President to enact certain sanctions against foreign persons found to be acting in support of the Government of Syria or other sanctioned individuals or groups operating in Syria. Specifically, Congress has required the President to sanction foreign individuals and entities who knowingly:

- provide financial, material, or technological support to: (i) the Government of Syria or a senior official; (ii) foreign military or paramilitary forces operating in Syria on behalf of the Syrian, Russian, or Iranian governments; or (iii) foreign persons already sanctioned under the United States’ Syria sanctions program;

- sell or provide “significant” goods, services, or any other support that “significantly facilitates” the Syrian Government’s natural gas or petroleum production;
- sell or provide aircraft or aircraft parts to foreign persons or forces operating in areas controlled by the Syrian government or otherwise associated with the Syrian government, or provides goods to services to any such foreign person;
- provide “significant” construction or engineering services to the Syrian government.

Additionally, the Act requires the Treasury Secretary to determine, by June 17, 2020, whether the Central Bank of Syria (“CBS”) constitutes an institution of primary money laundering concern under the USA PATRIOT ACT, a law enacted passed in 2001 to strengthen U.S. measures to prevent, detect, and prosecute international money laundering and terrorist financing. A primary money laundering concern designation would require U.S. banks that deal with the CBS to take certain information gathering and record-keeping measures and, more significantly, could result in U.S. banks’ being prohibited from opening or maintaining correspondent or payable-through accounts that involve the CBS. However, as of date of this writing no such determination appears to have been made.

Also on June 17, 2020, the U.S. Treasury and State Departments [designated 39 individuals](#) and entities under the Caesar Act and [Executive Order 13894](#) and one month later, on July 31, 2020, another 14 individuals and entities were [designated](#) under the same authorities. On June 5, 2020, OFAC [promulgated new regulations](#) implementing EO 13894 under [31 C.F.R. part 569](#). Interestingly, Syrian first lady Asma al-Assad and Assad’s adult son, Hafez al-Assad, were designated for the first time under this new authority. Syrian President Bashar al-Assad and other Syrian military officials were also named, but had previously been designated under authorities such as [EO 13573](#) and [EO 13582](#), which together provided for the designation of senior Syrian government officials and, more broadly, the Government of Syria. As we previously discussed in a [client alert](#) and [last year’s update](#), EO 13894 was initially enacted in October 2019 in order address Turkey’s aggression in northern Syria, rather than members of the Assad regime itself.

## D. North Korea

During the first half of 2020, the United States continued to mount pressure on the government of North Korea through the issuance of two separate sanctions advisories targeting the country’s illicit activities in the cyber and maritime sectors, amending and intensifying the North Korea Sanctions Regulations (“NKSr”), and bringing indictments against individuals for evading U.S. sanctions for the purpose of supporting the despotic regime’s nuclear program.

On April 15, the U.S. Departments of State, the Treasury, and Homeland Security, and the Federal Bureau of Investigation (“FBI”) issued an advisory on the [North Korean Cyber Threat](#) and on measures that the U.S. Government encourages industry and individuals to take to protect themselves from cyber-enabled malicious activity. The advisory notes that North Korea has increasingly relied upon cybercrime as a means to generate revenue in the face of mounting international sanctions. According to a UN sanctions committee expert report, North Korea has attempted to steal as much as U.S. \$2 billion through illicit cyber activities.

According to the advisory, cyberattacks sponsored by North Korean state-run organizations—including ransomware, spear phishing, and extortion campaigns—have targeted U.S. and international financial institutions, critical infrastructure, government and military networks, private industry, and individuals. Notable cyber incidents attributed to state-sponsored actors in North Korea include: the hacking of Sony Pictures in 2014, the theft of over \$80 million from Bangladesh Bank in 2016, and the WannaCry 2.0 ransomware attacks in 2017.

# GIBSON DUNN

The purpose of the advisory is to put industry and individuals on notice of the threat, to encourage commercial actors to adopt technical and behavioral measures to enhance their cybersecurity, and to encourage communication between industry and relevant U.S. Government agencies—including the [Cybersecurity and Infrastructure Security Agency](#) (“CISA”) and the [FBI Cyber Division](#).

Among the measures companies are encouraged to take is to implement appropriate anti-money laundering/countering the financing of terrorism/counter-proliferation financing compliance standards and programs, such as those published by the [Financial Action Task Force](#) or required, in the United States, under the Bank Secrecy Act. U.S. enforcement agencies, including FinCEN, are particularly concerned about U.S. financial institutions’ involvement in digital currency platforms that provide anonymous payment and account services without transaction monitoring, suspicious activity reporting or customer due diligence.

Separately, on April 10, 2020, OFAC [issued amendments](#) to the NKSR, found at 31 C.F.R. part 510. These amendments followed Congressional legislation focused on applying further pressure to the isolated regime’s stagnant economy, implementing provisions of the North Korea Sanctions and Policy Enhancement Act of 2016 (“NKSPEA”) (as amended by the Countering America’s Adversaries Through Sanctions Act (“CAATSA”) and the National Defense Authorization Act for Fiscal Year 2020 (“2020 NDAA”). The amendments made several changes to the NKSR, including: implementing secondary sanctions for certain transactions; adding potential sanctions restricting the use of correspondent accounts for non-U.S. financial institutions that have provided significant services to SDNs; prohibiting non-U.S. subsidiaries of U.S. financial institutions from transacting with the government of North Korea or any SDN designated under the NKSR; and revising the definitions of “significant transactions” and “luxury goods.” Due to the rather limited size of the North Korean economy, these changes may not have a very large practical effect; however, these changes serve to remind the international community of the risks involved when dealing with North Korea.

These risks were made even more apparent when, on May 28, 2020, DOJ unsealed an [indictment](#) charging 28 North Korean and 5 Chinese individuals, acting on behalf of North Korea’s Foreign Trade Bank, for facilitating over \$2.5 billion in illegal payments to support North Korea’s nuclear program. Though the prosecution is still in its early stages, the indictment is yet another reminder that U.S. enforcement agencies will continue to hold individuals and entities accountable—at times criminally accountable—for sanctions violations.

Rounding out the first half of the year, on July 16, 2020, OFAC [announced](#) that it had entered into a [settlement agreement](#) with UAE-based **Essentra FZE Company Limited** for violating the NKSR by exporting cigarette filters to North Korea using deceptive practices, including the use of front companies in China and elsewhere, and receiving payment into its accounts at a foreign branch of a U.S. bank. Significantly, OFAC found that Essentra FZE violated 31 C.F.R. § 510.212 by “causing” the U.S. bank to export financial services or engage in transactions involving North Korea. This enforcement action is reminiscent of OFAC’s 2017 settlement with CSE TransTel Pte. Ltd. (“TransTel”), a wholly owned subsidiary of CSE Global Limited (“CSE Global”). As we described in our [2017 Sanctions Year-End Update](#), OFAC in the CSE Global case appeared to expand its jurisdiction to cases in which non-U.S. parties “cause” U.S. entities (like financial institutions) to violate their sanctions obligations.

## II. New Developments

### A. China

Against the backdrop of the U.S.-China trade war, the United States has taken several



sanctions measures in recent months targeting China's aggression in its Xinjiang region and in Hong Kong. In a volatile political season, there is significant pressure in the U.S. Congress to take steps to deter China's alleged human rights abuses in its provinces, though it remains to be seen whether these sanctions measures will have any measurable economic impact. Moreover, recent weeks and months have seen a marked deterioration in the rhetoric used by the Trump administration to describe China's actions, and the Chinese government has taken retaliatory measures that so far have been deemed largely symbolic. China experts report these events as a "turning point" in the U.S.-China relationship and as a downward "ideological spiral" and new "cold war."

## **1. Human Rights & Forced Labor Concerns Regarding the Xinjiang Uyghur Autonomous Region**

In June and July, the government took several measures aimed at confronting and punishing China's alleged human rights abuses in the Xinjiang region. On June 17, 2020, the President signed the [Uyghur Human Rights Policy Act](#), which condemns actions taken by the government of China with respect to Turkic Muslims and other Muslim minority groups in the Xinjiang Uyghur Autonomous Region ("XUAR"). The Act requires the President to submit a report to Congress within 180 days that identifies foreign persons, including Chinese government officials, who are responsible for gross violations of human rights in Xinjiang, including, as identified in the legislation, torture, arbitrary detention, abduction, and the operation of internment and forced labor camps. The Act requires the imposition of blocking sanctions and a visa ban on persons identified in the report.

Shortly after passage of the Act, the U.S. Departments of State, Treasury, Commerce, and Homeland Security issued the [Xinjiang Supply Chain Business Advisory](#), a detailed guidance document for industry highlighting risks related to doing business with or connected to forced labor practices in Xinjiang and elsewhere in China. The Advisory states that businesses and individuals engaged in specified industries may face reputational or legal risks if their activities involve support for or acquisition of goods from commercial and governmental actors involved in illicit labor practices. The following activities were noted:

- Selling or providing biometric devices, cameras, computers, items with surveillance capabilities, microchips and microprocessors, tracking technology, or related equipment, software, and technology; and
- Involvement in joint ventures with PRC government officials and departments, or Chinese companies whose intellectual property has been known to aid the development or deployment of mass surveillance systems.

The Advisory recommends that businesses with supply chain links to Xinjiang assess their legal, economic, and reputational risks and take appropriate steps to implement reasonable human rights due diligence. The document provides many resources and links to internationally-recognized standards for conducting supply chain due diligence and establishing related corporate responsibility policies and procedures.

### ***Ratcheting Up Designations***

On July 9, OFAC [designated](#) the Xinjiang Public Security Bureau and four current and former senior officials of the Chinese Communist Party ("CCP") under authority delegated pursuant to the Global Magnitsky Act. The State Department [announced](#) complementary visa restrictions on three of the designated CCP officials. On July 31, the U.S. [designated](#) the Xinjiang Production and Construction Corps ("XPCC"), a paramilitary group associated with the CCP, as well as the XPCC's former Political Commissar and Deputy Party Secretary and Commander, also pursuant to the Global Magnitsky Act. We discuss the designation of other entities using U.S. export control authorities in Section IV.G, *supra*.

In response to the July 9 designations, on July 13, China [announced](#) “corresponding sanctions” against four U.S. officials and the U.S. Congressional-Executive Commission on China, an independent U.S. Government agency created by statute in 2001. Though these sanctions have widely been described as “symbolic,” it could portend further retaliatory action by China in the future.

## 2. Hong Kong

The U.S. Government has taken several measures in early 2020 in response to China’s crackdown on ongoing protests in Hong Kong, opposing China’s proposed legislation that would impose serious criminal penalties on activities deemed to constitute separatism, subversion or collusion with a foreign government.

On May 28, 2020, U.S. Secretary of State Michael Pompeo [reported](#) to Congress that Hong Kong no longer warrants preferential treatment under U.S. law as it no longer maintains a “high degree of autonomy” from mainland China. The “de-certification” was announced in conjunction with the State Department’s annual report on the status of Hong Kong required under the United States-Hong Kong Policy Act of 1992, as amended by the Hong Kong Human Rights and Democracy Act of 2019. On July 14, 2020, President Trump [issued](#) an Executive Order formally revoking Hong Kong’s special trading status. The effects of this de-certification and revocation are discussed further below in Section IV.F, *supra*.

The State Department also [announced](#) visa restrictions on current and former members of the CCP believed to be responsible for “undermining Hong Kong’s high degree of autonomy,” as guaranteed by the 1984 Joint Declaration signed by Great Britain and Hong Kong and governing the terms of the transfer of Hong Kong back to Chinese sovereignty. Under the Joint Declaration, Hong Kong was to retain unchanged its internal economic, political, and legal institutions through the transfer, effective July 1, 1997, for a period of fifty years until 2047.

### ***Hong Kong Autonomy Act authorizes additional sanctions***

After Beijing officials enacted the national security law on an accelerated basis, the U.S. Congress responded with legislation that would authorize the U.S. Government to impose sanctions on foreign persons determined to have materially contributed to the failure of China to meet its obligations under the Joint Declaration, or its implementation in Hong Kong’s Basic Law, establishing the rights and freedoms particular to Hong Kong. President Trump signed the [Hong Kong Autonomy Act](#) on July 14, 2020.

The legislation requires the Secretaries of State and the Treasury to submit a report to Congress within 90 days of enactment identifying persons who have materially contributed to China’s actions in apparent violation of the Joint Declaration or the Basic Law. Blocking sanctions and visa restrictions are required within one year of the report. The Secretaries of State and the Treasury are also required to report to Congress if they have determined that any foreign financial institutions have knowingly conducted a significant transaction with a person identified under the Act. Sanctions for financial institutions include asset freezes, bans on banking or correspondent account transactions with U.S. financial institutions, and sanctions on individual officers, among other restrictions.

## **B. Select Designations**

### **1. SDN List: Shanghai Saint Logistics Limited**

On May 19, 2020, OFAC [designated](#) the China-based Shanghai Saint Logistics Limited (“Shanghai Saint Logistics”) for acting as a general sales agent for Iranian commercial airline Mahan Air, an entity sanctioned by OFAC under counterterrorism authorities in



[October 2011](#) and by the State Department under antiproliferation authorities in [December 2019](#).

According to the U.S. Government, Mahan Air has, for years, transported terrorists and lethal cargo throughout the Middle East in support of Iran's Islamic Revolutionary Guard Corps ("IRGC") and the Assad regime in Syria. Mahan Air has also supported the Maduro regime by recently chartering flights to Venezuela for Iranian technicians and technical equipment (containing China-sourced materials).

As we pointed out in our [2019 Year-End Sanctions Update](#), OFAC's [July 2019 advisory](#) warned non-U.S. persons that they could face designation or secondary sanctions penalties for dealing with Mahan Air. And the year before, U.S. Secretary of the Treasury Steve Mnuchin [warned](#) the aviation industry to "sever all ties and distance themselves immediately from this airline." OFAC has backed up these warnings with action. In the past two years, OFAC has systematically targeted the non-U.S. actors supporting Mahan Air.

Shanghai Saint Logistics joins six other general sales agents ("GSAs") that have already been blacklisted by OFAC for dealing with Mahan Air. A GSA is an agent providing services on behalf of an airline, typically under the airline's brand. These services can include sales, marketing, freight handling, administrative services, and financial services. The now seven GSAs sanctioned for supporting Mahan Air span the globe, and include entities based in the [United Arab Emirates](#), [Malaysia](#), and [Thailand](#).

Unsurprisingly, the designation of Shanghai Saint Logistics has not been received well by the government the People's Republic of China ("PRC"). The PRC has [called](#) the designation "illegal" and has asked that the U.S. Government "change course and correct its mistake." As a PRC Foreign Ministry spokesperson put [it](#), "China stands consistently against U.S. unilateral sanctions and so-called long-arm jurisdiction."

## 2. Cuba Restricted List: FINCIMEX and Travel Companies

Consistent with President Trump's [mandate](#) to "identify the entities or subentities . . . that are under the control of, or act for or on behalf of, the Cuban military, intelligence, or security services or personnel," the State Department has maintained a List of Restricted Entities and Subentities Associated with Cuba (the "Cuba Restricted List") since November 2017. As we covered in our [November 16, 2017 client alert](#), OFAC generally [prohibits](#) U.S. persons and entities from engaging in direct financial transactions with those entities and subentities on the Cuba Restricted List. BIS also has a general [policy](#) of denying applications to export or reexport items for use by such listed entities and subentities.

On June 12, 2020, the State Department [added](#) seven Cuban military-owned subentities—most operating in Cuba's tourism industry—to the Cuba Restricted List: (1) a financial services company (FINCIMEX); (2) three hotels (Hotel Marqués de Cardenas de Montehermoso, Hotel Regis, Playa Paraíso Hotel); (3) two diving centers (Varadero, Gaviota Las Molas); and (4) a marine park for tourists (Cayo Naranjo dolphinarium). In [announcing](#) the additions, Secretary of State Pompeo stated that the profits generated by these seven subentities were being used to oppress the Cuban people and fund interference in Venezuela. A State Department senior official apparently [characterized](#) the additions as a "birthday present to Raul Castro" who turned 89 the day prior.

The listing of FINCIMEX, which handles remittances to Cuba and processes foreign-issued credit cards, is notable. FINCIMEX is the exclusive Cuban representative of Western Union, the vendor of choice for thousands of Americans who send money to their Cuban relatives. A Western Union spokesperson [stated](#) that, despite the FINCIMEX listing, "business and services from the U.S. to Cuba are operating as usual and [are] in compliance with U.S. law and regulations." At this stage, it remains to be seen to what degree remittances to Cuba will be affected in practice. At the very least, this development

is consistent with the Trump administration's recent attempts to tighten remittance-related allowances, such as imposing \$1,000 per quarter cap on remittances to Cuba as of September 2019. For more on these remittance-related restrictions, see our [2019 Year-End Sanctions Update](#).

### 3. Section 7031(c) Designations: Corrupt Actors and Human Rights Violators

Pursuant to Section 7031(c) of the Further Consolidated Appropriations Act of 2020, "[o]fficials of foreign governments and their immediate family members about whom the Secretary of State has credible information have been involved in significant corruption . . . or a gross violation of human rights [are] ineligible for entry into the United States." Section 7031(c) designations can be made public or kept private by the State Department. A variation of this authority has existed in annual State-Department appropriations legislation since 2008. However, the Trump administration was the first to implement it when it [publicly designated](#) an allegedly corrupt former Albanian prosecutor under Section 7031(c) in February 2018.

Since then, the Trump administration has not been shy about adding to the Section 7031(c) list. Currently, more than [150 individuals](#) (including immediate family members) from over thirty countries have been publicly designated. Thirty of these individuals were designated in the first three months of 2020. They include, for example: (1) [thirteen former military personnel from El Salvador](#) allegedly involved in the killing of six Jesuit priests and two others on November 16, 1989 on the campus of Central American University; (2) IRGC Commander [Hassan Shahvapour](#), whose military units killed as many as 148 Iranian protestors in November 2019; and (3) [Roberto Sandoval Castañeda](#), a former governor of the Mexican state of Nayarit, who misappropriated state assets and received bribes from narcotics trafficking organizations. Gibson Dunn will continue to monitor the use of Section 7031(c) designations, as well as other human-rights-based tools of foreign policy available to the President such as the Global Magnitsky sanctions.

## III. Other U.S. Developments

### A. International Criminal Court

As we have previously [noted](#), the Trump administration has deployed sanctions in unprecedented ways and directed their force at surprising targets. On June 11, the President, unilaterally and without coordination with the United States' European partners, issued an [Executive Order](#) authorizing sanctions against foreign persons determined to have engaged in any effort by the International Criminal Court ("ICC") to investigate, arrest, detain, or prosecute United States or any U.S. ally personnel without the consent of the United States or that ally. Previously, on March 5, the ICC announced that it would authorize its chief prosecutor to open an investigation into alleged war crimes committed in Afghanistan, including any that may have been committed by U.S. personnel. The Executive Order refers to this decision and reiterates that the United States is not a party to the Rome Statute and has not consented to ICC jurisdiction. To date, no designations have been made under the order.

This action is somewhat reminiscent of the quickly-implemented, and just as quickly removed, sanctions against Turkey in October 2019—the first time that sanctions had been used to target government ministries of a NATO-member country. Unlike the October 2019 sanctions against Turkey, however, it is unlikely that this order will be revoked in the near future. The June 11 Executive Order demonstrates the continued willingness of the Trump administration to use sanctions to advance political and policy interests that traditionally have been outside the conventional use of sanctions.

### B. New York Department of Financial Services

New York's Department of Financial Services ("DFS"), the state's key regulator in the financial industry, continues to bring enforcement actions against banks that have a New York presence for money laundering and sanctions violations. In its first action involving allegations of sanctions violations since its [\\$405 million fine against Unicredit Group in April 2019](#), on April 20, 2020, DFS [announced](#) a \$35 million dollar settlement with the Industrial Bank of Korea ("IBK") for its failure to maintain adequate Bank Secrecy Act and anti-money laundering ("AML") compliance programs. Among the compliance failures, DFS noted that IBK failed to detect a money laundering scheme that involved circumventing unspecified sanctions laws, with almost \$1 billion clearing through New York banks.

Later that month DFS [announced](#) a \$220 million settlement with Bank HaPoalim for knowingly facilitating clients' tax evasion, and in July the regulator [brought](#) a \$150 million action against Deutsche Bank for its failure to flag suspicious activities involving Jeffrey Epstein's accounts as well as its failure to adequately monitor the activities of its clients Danske Estonia and FBME Bank, despite known risks associated with both banks. These actions, together with the [appointment](#) of a new DFS General Counsel with extensive background in AML and sanctions compliance, indicate that the state regulator will continue to devote significant resources to sanctions and AML enforcement; financial institutions with a New York presence should take heed that OFAC is far from being the only agency monitoring this space.

## IV. Export Controls

Despite operating under work-from-home orders due to COVID-19 and a number of significant items still remaining on their to-do list, the staff at the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") has already had an extraordinarily busy year administering U.S. export controls on dual-use goods, software, and technology. BIS is continuing to evaluate how to identify and control exports of "emerging and foundational technologies," as required by the Export Control Reform Act of 2018, with anticipated controls on emerging technologies expected any day and new proposals for foundational technologies reportedly in the pipeline as well. In the meantime, BIS has imposed a number of significant new controls on trade with China and Hong Kong and has suggested that more may be on the way. Alongside these developments, BIS has continued the use of its powerful Entity List designation tool to effectively ban U.S. exports to entities implicated by the Executive Branch's interagency End-User Review Committee ("ERC") in certain human rights violations in the XUAR and elsewhere in China.

These developments demonstrate that BIS is continuing to move away from its past as a purely technical agency and towards a much more dynamic future in which its authorities are used for foreign policy and national security objectives, not unlike OFAC. In some respects this is because the collateral impact of an SDN designation on a large company, such as Huawei, is too significant and disruptive to the global economy, and the more limited impact on being added to the Entity or Unverified Lists is more palatable. As such, as the trade war with China heats up and the potential for more designations of even more economically consequential actors becomes a reality, the administration (and the next one) will likely continue to rely on these "lesser" restrictions in place of adding these too-big-to-sanction entities to the SDN blacklist.

### A. 0Y521 Series Classification for Geospatial SW

On January 3, BIS [announced](#) that it would be imposing new export controls on certain types of artificial intelligence software specially designed to automate the analysis of geospatial imagery in response to emergent national security concerns related to the newly covered software. Covered software includes products that employ artificial intelligence to analyze satellite imagery and identify user-selected objects. As a result of the new controls, a license from BIS is now required to export the geospatial imagery software to all countries, except Canada, or to transfer the software to foreign nationals.

The only exception to this license requirement is for software transferred by or to a department or agency of the U.S. Government.

Implementing new export controls can often be a lengthy process, sometimes requiring international coordination. However, to implement this new license requirement, BIS deployed a rarely used tool for temporarily controlling the export of emerging technologies—the 0Y521 Export Controls Classification Number (“ECCN”). This special ECCN category allows BIS to impose export restrictions on previously uncontrolled items that have “significant military or intelligence advantage” or when there are “foreign policy reasons” supporting restrictions on its export. Although these controls would only last one year, items subjected to these controls can be moved to a more permanent ECCN before the expiration of the classification.

These controls on covered geospatial imagery software will last at least until January 2021, and the United States will work with its allies over the course of 2020 to impose permanent, multilateral controls on this software. As noted above, we are also expecting BIS to publish a suite of new controls on “emerging technologies” in the near future. BIS has also indicated that it hopes to soon publish an Advanced Notice of Proposed Rulemaking on “foundational” technologies.

## **B. Expansion of Military End Use/User Rule**

In response to U.S. Government concerns about significant overlap between the development of China’s military and commercial sectors, BIS announced a range of regulatory changes on April 28. The most significant of these changes was the expansion of U.S. controls on exports of items to military end users or for military end uses. Specifically, the new rule, which was implemented on June 29, strengthens the controls on exports to China, Russia, and Venezuela by:

- Expanding the definition of “military end uses” for which exports must be authorized;
- Adding a new license requirement for exports to Chinese “military end users”;
- Expanding the list of products to which these license requirements apply; and
- Broadening the reporting requirement for exports to China, Russia, and Venezuela.

### **1. Expanding Military End Uses Subject to Control**

Exporters of certain goods, software, or technology that are subject to the Export Administration Regulations (“EAR”) previously required a license from BIS to provide those items to China, Russia, or Venezuela if the exporters knew or had reason to know that the items were intended, entirely or in part, for a “military end use” in those countries. This licensing requirement is separate from the EAR’s item-based licensing requirements that otherwise identify which items require export licenses when exported to specific countries and which are based on a range of national security and foreign relations policies. Under the separate, military end use and end user license requirement, “military end use” was defined to include the “use,” “development,” or “production” of certain military items. An export was considered to be for the “use” of a military item if the export is for the operation, installation, maintenance, repair, overhaul and refurbishing of the military item. The exported item had to perform all six functions in order to be considered a “use” item subject to the military end use restriction.

The new rule expands the definition of “military end use” in two important ways. Where the prior formulation only captures items exported for the purpose of using, developing, or producing military items, the revised rule also captures items that merely “support or contribute to” those functions. The revised rule also effectively broadens the definition of “use.” Rather than requiring that an item perform all six previously listed functions, an item that supports or contributes to any one of those functions will now be subject to the military

end use license requirement. For example, a repair part for a military item that might not have required a license under the previous formulation (perhaps because it was not also required for the military item's installation) would be subject to the updated license requirement.

## 2. Restricting Exports to Chinese Military End Users

Under the prior regulations, exports to military end users in Russia and Venezuela were subject to a specific license requirement. The new rule now also require licenses for exports of covered items to Chinese military end users.

Military end users covered by this license requirement not only include national armed services, police, and intelligence services, but also include "any person or entity whose actions or functions are intended to support 'military end uses.'" Taken together with the newly broadened definition of "military end uses," this restriction may apply to a significant number of private entities in China, even those that are engaged largely in civilian activities. For example, a manufacturing company that has an unrelated contract with a military entity could be considered a "military end user" subject to these strict licensing requirements. Given that applications for BIS licenses to export covered items for military end uses or end users face a presumption of denial, this restriction could have a significant impact on commerce with large swaths of the Chinese economy, where the U.S. Government has indicated its concerns about military-civilian collaboration in Chinese industry.

## 3. Expanding the List of Covered Items

The updated rule also expands the category of goods, software, or technology that require a license for military end use or end user exports. The previous military end use/end user license requirement applied to a relatively limited set of items specifically described in a supplement to the rule. The revised rule expands the scope of the item categories already listed and adds many new categories of covered items—including goods, technology, and software relating to materials processing, electronics, telecommunications, information security, sensors and lasers, and propulsion.

Many of the new items were previously subject to some of the EAR's most permissive controls and did not generally require a license for export to China, Russia, or Venezuela. For example, mass market encryption software (ECCN 5D992)—a category which includes many types of software that incorporate or call on common encryption functionality—were not previously subject to the military end use restrictions but now are subject to the new controls.

## 4. Broadening the Reporting Requirement

BIS is also now requiring exporters to report more often and to provide more data on items provided to China, Russia, or Venezuela.

Under the previous rules, exporters were not required to provide Electronic Export Information ("EEI") for shipments valued under \$2,500. Exporters also were not required to provide the ECCN for shipments of items that were only controlled for export because of antiterrorism concerns—the most permissive and most frequently applied category of control on the EAR's list of items controlled for export.

Under the new rules, there is no value threshold. EEI is generally required for all shipments to China, Russia, or Venezuela of items described on the Commerce Control List (CCL) regardless of value (i.e., all items except those classified EAR 99). Moreover, exporters are required to provide the ECCNs for all items exported to China, Russia, or Venezuela, regardless of the reason for control.

In announcing this change, U.S. Commerce Secretary Wilbur Ross [noted](#) that "[c]ertain

entities in China, Russia, and Venezuela have sought to circumvent America's export controls, and undermine American interests in general." Secretary Ross vowed that the United States would "remain vigilant to ensure U.S. technology does not get into the wrong hands." This amendment to the EEI reporting requirements—along with the other new licensing requirements—is designed to ensure that BIS and other U.S. Government trade enforcement agencies have increased visibility into shipments to jurisdictions of significant concern.

## C. Removal of License Exception for Civilian End Use

On June 29, BIS also [removed](#) License Exception Civil End Users ("CIV") from Part 740 of the EAR. This exception previously allowed eligible items controlled only for National Security (NS) reasons to be exported or reexported without a license for civil end users and civil end uses in countries included in Country Group D:1, excluding North Korea. NS controls are BIS's second most frequently applied type of control, applying to a wide range of items listed in all categories of the CCL. Country Group D:1 identifies countries of national security concern for which the Commerce Department will review proposed exports for potential contribution to the destination country's military capability. D:1 countries include China, Russia, Ukraine, and Venezuela, among others.

By removing License Exception CIV, the Commerce Department now requires a license for the export of items subject to the EAR and controlled for NS reasons to D:1 countries. As with the expansion of the military end use/end user license requirements described above, the Commerce Department has stated that the reason for the removal of License Exception CIV is the increasing integration of civilian and military technological development pursued by countries identified in Country Group D:1, making it difficult for exporters or the U.S. Government to be sufficiently assured that U.S.-origin items exported for apparent civil end uses will not actually also be used to enhance the military capacity contrary to U.S. national security interests.

## D. Proposed Amendment of License Exception APR

BIS also [proposed to amend](#) the EAR's License Exception Additional Permissive Reexports ("APR"), which currently allows the unlicensed reexport (the export of a U.S.-origin item from one non-U.S. country to another non-U.S. country) of an item subject to the EAR from trusted allies with similar export control regimes (i.e., listed in Country Group A:1, and Hong Kong) to countries presenting national security concerns (i.e., Country Group D:1, except North Korea). To be eligible for the exception, the reexport must also be consistent with the export licensing policy of the reexporting country and the item must be subject to only a subset of other controls (i.e., controlled only for antiterrorism, national security, or regional security reasons), among other limitations. The reexporting countries identified in Country Group A:1 include those countries that are participants with the United States in the Wassenaar Arrangement, a multilateral consortium that develops export controls on conventional weapons and dual-use items and underlies much of the U.S. export control regime. BIS's proposed amendment would remove this portion of the license exception.

The Commerce Department explained that it has proposed this amendment because of concerns regarding variations in how the United States and its international partners, including those in Country Group A:1, perceive the threat caused by the policy of civil-military technological integration pursued by D:1 countries. Due to these alleged disparities, reexports under License Exception APR have occurred that reportedly would not have been licensed by BIS if the export had taken place directly from the United States.

This proposed rule change echoes recent changes affecting the scope of investment reviews by the U.S. Committee on Foreign Investment in the United States ("CFIUS"), by which the United States has similarly sought to incentivize foreign allies to harmonize their



national security-related measures with those of the United States. In the new CFIUS rules implemented in February and previously described [here](#), the Committee will require “excepted foreign states” to ensure their national security-based foreign investment review process meets requirements established by CFIUS in order to retain their excepted status.

## E. Huawei Direct Product Rule

In addition to the broad new restrictions on Chinese trade described above, the United States has also focused specifically on restricting trade with Huawei Technologies Co. Ltd. (“Huawei”)—one of the world’s largest technology companies—on the basis of concerns about espionage and national security risks that U.S. officials allege its products may present. Among other U.S. Government initiatives to dissuade U.S. allies from partnering with Huawei and other Chinese telecommunications providers in the development and deployment of 5G networks, BIS has designated Huawei and over one hundred of its affiliates to the Entity List, which has significantly limited Huawei’s ability to source many products directly from the United States and the non-U.S. affiliates of many U.S. companies.

On May 15, BIS [announced](#) a new rule to further restrict Huawei’s access to U.S. technology. The rule amends the “Direct Product Rule” and the BIS Entity List to restrict Huawei’s ability to share its semiconductor designs or rely on foreign foundries to manufacture semiconductors using U.S. software and technology.

Although Huawei’s Entity List designation had already effectively cut off Huawei’s access to exports of most U.S.-origin products and technology, BIS has claimed that Huawei has responded to the designations by moving more of its supply chain outside the United States. Huawei and many of the foreign chip manufacturers that Huawei uses, however, still depend on U.S. equipment, software, and technology to design and produce Huawei chipsets.

BIS’s action expands one of the bases on which the U.S. can claim jurisdiction over items produced outside of the United States. Generally, under the EAR, the U.S. claims jurisdiction over items that (1) are U.S. origin; (2) foreign-made items that are being exported from the U.S., (3) foreign-made items that incorporate more than a minimal amount of controlled U.S.-origin content, and (4) foreign-made “direct products” of certain controlled U.S.-origin software and technology. Under the fourth basis of jurisdiction, also known as the Direct Product Rule, foreign-made items are subject to EAR controls if they are the direct product of certain U.S.-origin technology or software or are the direct product of a plant or major component of a plant located outside the U.S., where the plant or major component of a plant itself is a direct product of certain U.S.-origin software and technology. Items that are subject to EAR controls may require BIS licensing depending on the export classification of the item and its destination, the end use to which the item is being put, and the end user receiving it. Depending on the licensing policy BIS applies to particular exports, BIS can effect an embargo on the export of items subject to the EAR to particular countries, end uses, and end users.

BIS’s new rule allows for the application of a tailored version of the Direct Product Rule to parties identified on its Entity List, with a bespoke list of controlled software and technology commonly used by foreign manufacturers to design and manufacture telecommunications and other kinds of integrated circuits for Huawei. The rule imposes a control on foreign-produced items that are a direct product of an expanded subset of specific technology or software described by certain specified ECCNs and foreign-produced items that are the direct product of a plant or major component of a plant located outside the U.S. where the plant or major component is a direct product of the same expanded subset of U.S.-origin technology or software.

Specifically, the rule will make the following non-U.S.-origin items subject to the

restrictions of U.S. export controls:

- Items, such as chip designs, that Huawei and its affiliates on the Entity List produce by using certain software or technology that is subject to the EAR; and
- Items, such as chipsets made by manufacturers from Huawei-provided design specifications, if those manufacturers are using semiconductor manufacturing equipment that itself is a direct product of certain software or technology subject to the EAR.

Combined with Huawei's Entity List designation, this new rule will significantly restrict Huawei's ability to export its semiconductor designs as well as to receive semiconductors from its foreign manufacturers. It will also curtail the ability of Huawei to receive semiconductors from the non-U.S. subsidiaries of U.S. companies that may have previously been eligible for export to Huawei without a license because they were produced from software and technology that would not have triggered export licensing through the normal operation of the Direct Product Rule. Taken together, these changes mean that BIS can now block the sale of many semiconductors manufactured by a number of non-U.S.-based manufacturers that Huawei uses across its telecom equipment and smartphone business lines.

## F. Revoking Hong Kong's Status under U.S. Export Controls

In response to China's Hong Kong National Security Law—which the Trump administration considers an encroachment on Hong Kong's special status—President Trump [announced](#) on May 29 that the U.S. would reevaluate its export controls imposed on Hong Kong to revoke any preferential treatment given the territory over mainland China. A month later, following statements by Secretaries [Pompeo](#) and [Ross](#), BIS announced that it would be [suspending](#) license exceptions that treated Hong Kong differently than mainland China. The agency has not yet made any other adjustments to the treatment of Hong Kong-bound exports or to license exceptions that apply equally to Hong Kong and mainland China—although an [Executive Order](#) announced on July 14 will likely require further leveling of treatment for exports to Hong Kong and mainland China.

As a result of the license exception suspension enacted on June 30, license exceptions that previously permitted unlicensed exports, reexports, or transfers to or within Hong Kong, but not to mainland China, no longer authorizes exports to Hong Kong. Such exports will now require specific authorization from BIS. For example, exports to Hong Kong of software and technology related to telecommunications equipment that would have previously been authorized under License Exception – Technology and Software under Restriction (“[TSR](#)”) may now require a specific license. Deemed exports (i.e., the transfer of technology or source code to a foreign person in the U.S.) may continue under affected licenses until August 28.

Other license exceptions affected (but not necessarily unavailable) may include those pertaining to replacement of parts and equipment (“[RPL](#)”), aircraft, vessels, and spacecraft (“[AVS](#)”), gifts (“[GFT](#)”), and baggage (“[BAG](#)”). Importantly the suspension of these license exceptions would not impact products that are not subject to the EAR (e.g., by virtue of their place of development or delivery only through the cloud), are specifically authorized by a BIS-issued license, or are authorized by a license exception that applies equally to both Hong Kong and mainland China.

## G. Human Rights-Based Entity List Designations

As we highlighted in our [2019 Year End Review](#), the ERC, which is chaired by BIS, has been exceptionally active over the past several years. While the ERC, which is composed of representatives of Departments of Commerce, State, Defense, Energy and, where appropriate, the Treasury, has always had the power to designate companies and other organizations for acting counter to U.S. national security and foreign policy interests, these

# GIBSON DUNN

interests historically have been focused on regional stability, counterproliferation, and anti-terrorism concerns and violators of U.S. sanctions and export controls. Beginning in October last year, however, the ERC added human rights to this list of concerns, particularly as they relate to human rights violations occurring in the XUAR and other regions of China directed Uyghurs, Kazakhs, and other members of Muslim minority groups in China.

On October 9, 2019, the ERC placed the XUAR People's Government Public Security Bureau, eighteen of its subordinates, and an additional eight businesses on its Entity List, thereby restricting their access to American exports. On June 5, 2020, BIS placed eight additional businesses and one governmental institute on the Entity List on the explicit basis of their human rights violations. Those added to the Entity List are largely surveillance or security companies, including certain artificial intelligence start-ups. Most recently, on July 22, BIS designated eleven additional entities. Nine appear to be in the apparel, accessories, and manufacturing sectors and were designated due to the ERC's finding that they were using forced labor. Two other entities were added for their involvement in conducting genetic analyses used to further the repression of Muslim minority groups in the XUAR.

As a result of these designations, almost all exports of items subject to the EAR require BIS's prior review and authorization and most are subject to a policy presumption of denial.

---

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Adam Smith, Stephanie Connor, Chris Timura, Jesse Melman, R.L. Pratt, Scott Toussaint, Samantha Sewall and Audi Syarief.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding the above developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any of the following leaders and members of the firm's International Trade practice group:

## **United States:**

Judith Alison Lee – Co-Chair, International Trade Practice, Washington, D.C. (+1 202-887-3591, [jalee@gibsondunn.com](mailto:jalee@gibsondunn.com))  
Ronald Kirk – Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, [rkirk@gibsondunn.com](mailto:rkirk@gibsondunn.com))  
Jose W. Fernandez – New York (+1 212-351-2376, [jfernandez@gibsondunn.com](mailto:jfernandez@gibsondunn.com))  
Marcellus A. McRae – Los Angeles (+1 213-229-7675, [mmcrae@gibsondunn.com](mailto:mmcrae@gibsondunn.com))  
Adam M. Smith – Washington, D.C. (+1 202-887-3547, [asmith@gibsondunn.com](mailto:asmith@gibsondunn.com))  
Stephanie L. Connor – Washington, D.C. (+1 202-955-8586, [sconnor@gibsondunn.com](mailto:sconnor@gibsondunn.com))  
Christopher T. Timura – Washington, D.C. (+1 202-887-3690, [ctimura@gibsondunn.com](mailto:ctimura@gibsondunn.com))  
Ben K. Belair – Washington, D.C. (+1 202-887-3743, [bbelair@gibsondunn.com](mailto:bbelair@gibsondunn.com))  
Courtney M. Brown – Washington, D.C. (+1 202-955-8685, [cmbrown@gibsondunn.com](mailto:cmbrown@gibsondunn.com))  
Laura R. Cole – Washington, D.C. (+1 202-887-3787, [lcoble@gibsondunn.com](mailto:lcoble@gibsondunn.com))  
Jesse Melman – New York (+1 212-351-2683, [jmelman@gibsondunn.com](mailto:jmelman@gibsondunn.com))  
R.L. Pratt – Washington, D.C. (+1 202-887-3785, [rpratt@gibsondunn.com](mailto:rpratt@gibsondunn.com))  
Samantha Sewall – Washington, D.C. (+1 202-887-3509, [ssewall@gibsondunn.com](mailto:ssewall@gibsondunn.com))  
Audi K. Syarief – Washington, D.C. (+1 202-955-8266, [asyarief@gibsondunn.com](mailto:asyarief@gibsondunn.com))  
Scott R. Toussaint – Washington, D.C. (+1 202-887-3588, [stoussaint@gibsondunn.com](mailto:stoussaint@gibsondunn.com))  
Shuo (Josh) Zhang – Washington, D.C. (+1 202-955-8270, [szhang@gibsondunn.com](mailto:szhang@gibsondunn.com))

## **Europe:**

Peter Alexiadis – Brussels (+32 2 554 72 00, [palexiadis@gibsondunn.com](mailto:palexiadis@gibsondunn.com))  
Attila Borsos – Brussels (+32 2 554 72 10, [aborsos@gibsondunn.com](mailto:aborsos@gibsondunn.com))  
Nicolas Autet – Paris (+33 1 56 43 13 00, [nautet@gibsondunn.com](mailto:nautet@gibsondunn.com))  
Susy Bullock – London (+44 (0)20 7071 4283, [sbullock@gibsondunn.com](mailto:sbullock@gibsondunn.com))  
Patrick Doris – London (+44 (0)207 071 4276, [pdoris@gibsondunn.com](mailto:pdoris@gibsondunn.com))  
Sacha Harber-Kelly – London (+44 20 7071 4205, [sharber-kelly@gibsondunn.com](mailto:sharber-kelly@gibsondunn.com))

# GIBSON DUNN

Penny Madden – London (+44 (0)20 7071 4226, [pmadden@gibsondunn.com](mailto:pmadden@gibsondunn.com))

Steve Melrose – London (+44 (0)20 7071 4219, [smelrose@gibsondunn.com](mailto:smelrose@gibsondunn.com))

Matt Aleksic - London (+44 (0)20 7071 4042, [maleksic@gibsondunn.com](mailto:maleksic@gibsondunn.com))

Benno Schwarz – Munich (+49 89 189 33 110, [bschwarz@gibsondunn.com](mailto:bschwarz@gibsondunn.com))

Michael Walther – Munich (+49 89 189 33-180, [mwalther@gibsondunn.com](mailto:mwalther@gibsondunn.com))

Richard W. Roeder – Munich (+49 89 189 33-160, [rroeder@gibsondunn.com](mailto:rroeder@gibsondunn.com))

© 2020 Gibson, Dunn & Crutcher LLP, 333 South Grand Avenue, Los Angeles, CA 90071

Attorney Advertising: The enclosed materials have been prepared for general informational purposes only and are not intended as legal advice.

## **Related Capabilities**

[International Trade Advisory and Enforcement](#)

[Financial Institutions](#)

[Mergers and Acquisitions](#)