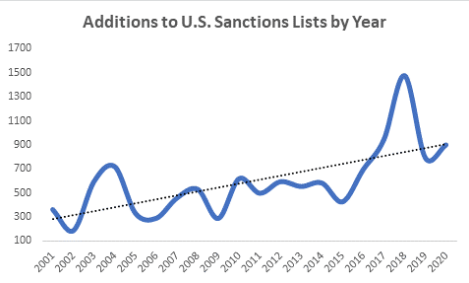
GIBSON DUNN

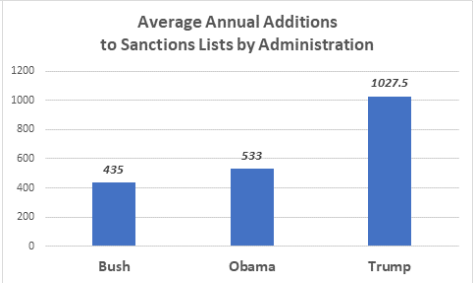
2020 Year-End Sanctions and Export Controls Update

Client Alert | February 5, 2021

2020 was a uniquely uncertain and perilous year. Within the world of international trade, the steady increase in the use of sanctions and export controls—principally by the United States but also by jurisdictions around the world—proved to be a rare constant. In each of the last four years, our annual year-end Updates have chronicled a sharp rise in the use of sanctions promulgated by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), as well as growing economic tensions between the United States and other major world powers. In the final tally, OFAC during President Donald Trump's single term sanctioned more entities than it had under two-term President George W. Bush and almost as many as two-term President Barack Obama.

The raw numbers understate the story, as the Trump administration focused sanctions authorities on larger and more systemically important players in the global economy than ever before, and also brought to bear other coercive economic measures—including export controls, import restrictions, foreign investment reviews, tariffs, and novel measures like proposed bans on Chinese mobile apps and restrictions on U.S. persons' ability to invest in securities of certain companies with alleged ties to the Chinese military. The pace and frequency of these actions intensified in the Trump administration's final days—an ostensible attempt to force the hand of the incoming Biden-Harris administration on a number of key national security policy decisions.





China takes top billing in this year's Update, as long-simmering tensions between Beijing and Washington seemingly reached a boil. Despite a promising start to the year with the January 2020 announcement of a "phase one" trade agreement between the world's two largest economies, relations between the two powers rapidly deteriorated amidst recriminations concerning the pandemic, a crackdown in Hong Kong, a heated U.S. presidential election, and a deepening struggle for economic, technological, and military primacy. The Chinese government on January 9, 2021 responded to the Trump administration's barrage of trade restrictions by issuing the first sanctions blocking regime in China to counteract the impact of foreign sanctions on Chinese firms. Although the law—which borrows from a similar measure adopted by the European Union—is effective immediately, it currently only establishes a legal framework. The Chinese blocking statute will become enforceable once the Chinese government identifies the specific extra-territorial measures—likely sanctions and export controls the United States has levied against Chinese companies—to which it will then apply. While experts have long predicted

Related People

Judith Alison Lee

Attila Borsos

Patrick Doris

Markus Nauheim

Adam M. Smith

Wilhelm Reinhardt

Qi Yue

Christopher T. Timura

John Matthew Butler

Anna Helmer

Allison Lewis

Sonja Ruttmann

Anna Searcey

Audi K. Syarief

Scott R. Toussaint

Shuo Josh Zhang

Samantha Sewall

the rise of a technological Cold War with Chinese 5G and Western 5G competing for dominance—the advent of China's blocking statute (amid threats of additional counter-measures) suggests the emergence of a regulatory Cold War as well. Major multinational companies may be forced to choose between the two powers.

The pandemic and Sino-American tensions almost over-shadowed what would have been the principal trade story of the year: nearly four-and-a-half years after the United Kingdom voted to leave the European Union, London and Brussels finally completed Brexit. On December 30, 2020—one day prior to the end of the Brexit Transition period—the EU and China concluded negotiations, over the objections of the incoming U.S. administration, for a comprehensive agreement on investment focused on enabling an increase in outbound investment in China from the EU.

At year's end, China, France, Germany, Russia, the United Kingdom, and the High Representative of the European Union for Foreign Affairs and Security Policy stressed the importance of the 2015 Joint Comprehensive Plan of Action ("JCPOA"), while the Trump administration sought to impose additional sanctions on Tehran that will make it more difficult for the Biden-Harris administration to reenter the agreement.

In the coming months, the Biden-Harris administration has promised a fulsome review of U.S. trade measures with a view to finding ways of providing possible relief to help with the global response to the coronavirus pandemic. And although we expect a more measured approach to diplomatic relations under the new administration, U.S. sanctions and export controls will continue to play a dominant role in U.S. foreign policy—and an increasingly dominant role in foreign policy strategies of America's friends and competitors. The increasing complexity of these measures in the United States—with "sanctions" authorities increasingly split between the U.S. Treasury Department, the Department of Commerce, the Department of State, the Department of Homeland Security, and even the Department of Defense—makes for increasing challenges for parties seeking to successfully comply while managing their businesses.

Contents

I. U.S.-China Relationship

The dozens of new China-related trade restrictions announced in 2020 were generally calculated to advance a handful of longstanding U.S. policy interests for which there is broad, bipartisan support within the United States, namely protecting U.S. communications networks, intellectual property, and sensitive personal data; slowing the advance of China's military capabilities; promoting human rights in Hong Kong and Xinjiang; and narrowing the trade deficit between Washington and Beijing. As such, while the new Biden-Harris administration promises a shift in tone—including greater coordination with traditional U.S. allies and a more orderly and strategic policymaking process—the core objectives of U.S. trade policy toward China are unlikely to change, at least in the near term. Given the emerging consensus in Washington in favor of a tough stance against China, we anticipate that President Biden will continue to pressure China over its human rights record and will be disinclined to relax Trump-era measures targeting Chinese-made goods and technology without first extracting concessions from Beijing.

Meanwhile, China shows few signs of backing down in the face of U.S. pressure. As we wrote here, in January 2021 China's Ministry of Commerce unveiled long-anticipated counter-sanctions prohibiting Chinese citizens and companies from complying with "unjustified" foreign trade restrictions, which could soon force multinational firms into an unpalatable choice between complying with U.S. or Chinese regulations. How vigorously and selectively the Chinese authorities enforce these new counter-sanctions remains to be seen and will help set the tone for the future of U.S.-China trade relations and the challenges multinational corporations will have in navigating between the two powers.

A. Protecting Communications Networks and Sensitive Personal Data

Spurred by concerns about Chinese espionage and trade secret theft, the United States during 2020 imposed a variety of trade restrictions designed to protect U.S. communications networks and sensitive personal data by targeting globally significant Chinese technology firms like ***Huawei*** and popular mobile apps like ***TikTok*** and ***WeChat***.

During 2020, the Trump administration continued its diplomatic, intelligence-sharing, and economic pressure campaign to dissuade countries from partnering with Huawei and other

Chinese telecommunications providers in the development and deployment of fifth-generation ("5G") wireless networks. The rollout of 5G networks—long viewed as a key battleground in the U.S.-China tech war—is about more than faster smartphones, as 5G networks are expected to support advanced technology like autonomous vehicles and to catalyze innovation across the economy from manufacturing to the military. As Huawei has emerged as a leader in 5G infrastructure, the U.S. government has increasingly raised alarms that the company's technology may be vulnerable to Chinese government espionage. Some U.S. allies have taken steps to block Huawei's involvement in their own domestic 5G networks. Australia blacklisted Huawei from its 5G network in August 2018, and the British government announced in July 2020 that it would ban the purchase of new Huawei equipment and would remove Huawei gear already installed from its networks by 2027, marking a reversal from a prior decision in January 2020. Other European allies, however, have resisted an outright ban, with Germany signaling in December 2020 that it could allow Huawei's continued involvement subject to certain assurances.

The Trump administration also continued to tighten the screws on Huawei along several other fronts, with the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") adding another 38 non-U.S. affiliates of Huawei to the Entity List in August 2020. Since first adding Huawei in May 2019 citing national security concerns, the Trump administration has added over 150 Huawei affiliates to the Entity List, significantly limiting Huawei's ability to source products from the United States and U.S. companies. These actions highlight the administration's sustained focus on Huawei, but also reflect a broader trend in the increasingly expansive use of the Entity List against Chinese firms. In its expanding size, scope, and profile, the Entity List has begun to rival the more traditional OFAC Specially Designated Nationals ("SDN") and Blocked Persons List as a tool of first resort when U.S. policymakers seek to wield coercive authority especially against major economies and significant economic actors.

On May 15, 2020, BIS announced a new rule to further restrict Huawei's access to U.S. technology. The complicated rule amends the "Direct Product Rule" (discussed below) and the 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 multiple rounds of Entity List designations targeting Huawei entities had already effectively cut off the company's access to exports of most U.S.-origin products and technology, BIS claimed that Huawei had responded to the designations by moving more of its supply chain outside the United States. However, for the time being, Huawei and many of the foreign chip manufacturers that Huawei uses, still depend on U.S. equipment, software, and technology to design and produce Huawei chipsets.

BIS's May 2020 Direct Product Rule amendment expanded 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 United States claims jurisdiction over items that are (1) U.S. origin, (2) foreign-made items that are being exported from the United States, (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 U.S. Export Administration Regulation ("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 United States, where the plant or major component of a plant itself is a direct product of certain U.S.-origin software and technology.

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. Specifically, the rule makes 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 U.S.-origin 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 U.S.-origin software or technology subject to the EAR.

By subjecting these items to a new licensing requirement, BIS can 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.

While Huawei has been a focal point of U.S. trade policy over the past several years, U.S. government concerns about maintaining the integrity of its communications networks and U.S. residents' sensitive personal data extend more broadly across China's tech sector. On May 15, 2019, acting under the authorities provided by the International Emergency Economic Powers Act ("IEEPA")—the statutory basis for most U.S. sanctions programs—President Trump issued Executive Order 13873, which declared a national emergency with respect to the exploitation of vulnerabilities in information and communications technology and services ("ICTS") by foreign adversaries, and authorized the Secretary of Commerce to prohibit transactions involving ICTS designed, developed, manufactured, or supplied by persons owned, controlled, or subject to the jurisdiction of a foreign adversary that pose an undue or unacceptable risk to U.S. critical infrastructure, the U.S. digital economy, national security, or the safety of U.S. persons.

On January 19, 2021, the Commerce Department published an Interim Final Rule clarifying the processes and procedures that the Secretary of Commerce will use to evaluate ICTS transactions covered by Executive Order 13873. The Interim Final Rule identified six foreign adversaries: China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Venezuela's President Nicolás Maduro; though this list can be revised as necessary. The Interim Final Rule also identified broad categories of ICTS transactions that fall within its scope, and announced that the Commerce Department will establish a licensing process for entities to seek pre-approval of ICTS transactions. Unless the Biden-Harris administration acts to delay the measure, the Interim Final Rule is scheduled to take effect on March 22, 2021.

B. TikTok and WeChat Prohibitions and Emerging Jurisprudence Limiting Certain Executive Authorities

To address the national emergency declared in the ICTS order, President Trump on August 6, 2020 issued two further Executive Orders restricting U.S. persons from dealing with the Chinese social media platforms TikTok and WeChat. The orders sought to prohibit or restrict certain categories of transactions—subsequently to be defined by the U.S. Secretary of Commerce—involving TikTok's corporate parent ***ByteDance*** and WeChat's corporate parent ***Tencent Holdings Ltd.*** by September 20, 2020.

Pursuant to these Executive Orders, the Commerce Department on September 18, 2020 issued a broad set of prohibitions that would have essentially banned the use or download of the TikTok and WeChat apps in the United States. The following day, a California federal district court granted a nationwide preliminary injunction halting the WeChat ban on First Amendment grounds. The plaintiffs, a group of WeChat users, successfully argued that WeChat functions as a "public square" for the Chinese-American community in the United States and that the restrictions imposed by the Commerce Department infringed upon their First Amendment rights.

One week later, a Washington D.C. federal district court granted a similar injunction with respect to the TikTok ban, finding that content exchanged by users on TikTok constitutes "information and informational materials" protected by the Berman Amendment, a

statutory provision within IEEPA that aims to safeguard the free flow of information. The court further found that, by virtue of being primarily a conduit of such informational materials, the platform itself was protected by the Berman Amendment. On October 30, 2020, a Pennsylvania federal district court granted a second, nationwide preliminary injunction halting the TikTok ban on Berman Amendment grounds. On December 7, 2020, the D.C. district court found that the Trump administration had overstepped its authority under IEEPA by failing to adequately consider "an obvious and reasonable alternative" to an outright ban. Together these opinions have clarified and expanded case law regarding the limits of the President's authority under IEEPA.

The litigation over the Commerce Department's TikTok and WeChat bans upended a parallel effort by the U.S. Committee on Foreign Investment in the United States ("CFIUS")—the interagency committee tasked with reviewing the national security risks associated with foreign investments in U.S. companies—to force a divestiture of TikTok's U.S. operations. In 2019, CFIUS initiated a review of ByteDance's 2017 acquisition of the U.S. video-sharing platform Musical.ly in response to growing concerns regarding the use of data and censorship directed by the Chinese government. The CFIUS review culminated in an August 14, 2020 order directing ByteDance to divest its interest in TikTok's U.S. platform by November 12, 2020.

The Commerce restrictions and ensuing litigation threatened to derail CFIUS negotiations over the TikTok divestment—a matter made more challenging on August 28, 2020, when China retaliated with its own set of export controls requiring Chinese government approval for such a transaction. Although the U.S. Department of the Treasury announced an agreement in principle for the sale of TikTok on September 19, 2020, a final agreement proved elusive. Negotiations ground to a halt around the time of the U.S. presidential election, and CFIUS extended the deadline for a resolution three times by the end of the year before defaulting to a *de facto* continuation as the parties continue to negotiate.

None of these developments, however, appeared to dampen the Trump administration's drive to target leading Chinese technology companies. On January 5, 2021, President Trump issued another Executive Order requiring the Commerce Department to issue a more narrowly tailored set of prohibitions with respect to the Chinese mobile payment apps WeChat Pay, Alipay, QQ Wallet, as well as CamScanner, SHAREit, Tencent QQ, VMate, and WPS Office within 45 days (by February 19, 2021). Given the timing of the order, the Biden-Harris administration will ultimately be responsible for either implementing or revoking the ban, setting up an early test case for the Biden-Harris administration with respect to Trump-era restrictions on Chinese tech companies.

C. Slowing the Advance of China's Military Capabilities

Another key goal of the Trump administration's trade policy in 2020 was its attempt to blunt the development of China's military capabilities, including by restricting exports to Chinese military end uses and end users, adding military-linked firms to the Entity List, prohibiting U.S. persons from investing in the securities of dozens of "communist Chinese military companies," and proposing new rules that seek to eject Chinese firms from U.S. stock exchanges for failure to comply with U.S. auditing standards.

Over the past year, the Trump administration has heavily relied on export controls to deny Beijing access to even seemingly low-end U.S. technologies that might be used to modernize China's military. Pursuant to the Military End Use / User Rule, exporters of certain listed items subject to the EAR require a license from BIS to provide such items to China, Russia, or Venezuela, if the exporter knows or has reason to know that the exported items are intended for a "military end use" or "military end user." In April 2020, BIS announced significant changes to these military end use and end user controls that became effective on June 29, 2020. Notably, the new rules (1) expanded the scope of military end uses subject to control, (2) added a new license requirement for exports to Chinese military end users, (3) expanded the list of covered items, and (4) broadened the

reporting requirement for exports to China, Russia, and Venezuela. These changes appear to have been animated by concerns among U.S. policymakers that the targeted countries are each pursuing a policy of "military-civil fusion" that blurs the line between civilian and military technological development and applications of sensitive technologies.

In particular, where the prior formulation of the Military End Use / User Rule only captured items exported for the purpose of using, developing, or producing military items, the rule now covers items that merely "support or contribute to" those functions. The scope of "military end uses" subject to control was also expanded to include the operation, installation, maintenance, repair, overhaul, or refurbishing of military items. For a more comprehensive discussion of the new Military End Use / User Rule, please see our client alert on the subject, as well as our 2020 Mid-Year Sanctions and Export Controls Update.

The expanded Military End Use / User Rule has presented a host of compliance challenges for industry, prompting BIS in June 2020 to release a detailed set of frequently asked questions ("FAQs") addressing potential ambiguities in the rule and in December 2020 to publish a new, non-exhaustive Military End User List to help exporters determine which organizations are considered military end users. The more than 100 Chinese and Russian companies identified to date appear to be principally involved in the aerospace, aviation, and materials processing industries, which is consistent with the newly added categories of items covered under the rule. BIS has also continued to add new companies to the Military End User List.

Meanwhile, reflecting the recent significant expansion of the bases for additions to the Entity List, the U.S. Department of Commerce during 2020 announced three batches of Entity List designations tied to activities in support of China's military. Among those designated in June, August and December 2020 were more than 50 governmental and commercial organizations accused of procuring items for Chinese military end users, building artificial islands in the South China Sea, and supporting China's policy of "military-civil fusion"—including substantial enterprises like the Chinese chipmaker ***Semiconductor Manufacturing International Corporation ("SMIC")***. Such military-related designations have continued into January 2021 with the addition to the Entity List of ***China National Offshore Oil Corporation ("CNOOC")*** for its activities in the South China Sea, suggesting that the Entity List remains an attractive option for U.S. officials looking to impose meaningful costs on large non-U.S. firms that act contrary to U.S. interests while avoiding the economic disruption of designating such enterprises to OFAC's SDN List.

In addition to using export controls to deny the Chinese military access to sensitive technology, during 2020 the Trump administration and Congress deployed several other types of measures to deny the Chinese military, and the firms that support it, access to U.S. capital. On November 12, 2020, the Trump administration issued Executive Order 13959, which sought to prohibit U.S. persons from purchasing securities of certain Communist Chinese military companies ("CCMCs")—ostensibly civil companies that the U.S. Department of Defense alleges have ties to the Chinese military, intelligence, and security services, including enterprises with substantial economic footprints in the United States such as Hikvision and Huawei. A fuller description of the Order and its implications can be found in our November 2020 client alert.

As amended and interpreted to date by OFAC (which has been tasked with implementing and enforcing the Order), Executive Order 13959 seeks to prohibit U.S. persons from engaging in any transaction in publicly traded securities or any securities that are derivative of, or are designed to provide investment exposure to such securities, of any CCMC. The Order covers a wide range financial instruments linked to such companies, including derivatives (e.g., futures, options, swaps), warrants, American depositary receipts, global depositary receipts, exchange-traded funds, index funds, and mutual funds.

OFAC has published a list of the targeted CCMCs, providing additional identifying information about the CCMCs. U.S. persons holding covered securities of CCMCs

identified in the initial Annex of Executive Order 13959 must sell or otherwise dispose of those securities by the expiration of a wind-down period on November 11, 2021. As such, the new Biden-Harris administration has a period of time to review the prohibitions and propose further modifications.

In the months since it was issued, Executive Order 13959 has generated widespread confusion within the regulated community concerning what activities are (and are not) prohibited, prompting index providers to sever ties with named Chinese companies and a major U.S. stock exchange to reverse course multiple times on whether such companies should be de-listed. Indeed, despite a flurry of guidance from OFAC, there remains considerable uncertainty concerning which companies are covered by the Order, including how the restriction applies to companies whose names "closely match" firms identified by the U.S. government, as well as such companies' subsidiaries. In seeming recognition of the compliance concerns expressed by industry, OFAC has issued a general license delaying the Order's effective date with respect to entities with "closely matching" names of parties explicitly listed until May 2021.

Whatever comes of the Trump administration's restrictions on investments in CCMCs, there remains broad bipartisan support in Congress for denying Chinese firms access to U.S. capital markets. In December 2020, Congress unanimously passed and President Trump signed into law the Holding Foreign Companies Accountable Act, which requires foreign companies listed on any U.S. stock exchange to comply with U.S. auditing standards or risk being de-listed within three years. Although formally applicable to companies from any foreign country, the Act appears to be principally aimed at Chinese firms, many of which have historically declined to comply with U.S. auditing standards, citing national security and state-secrets concerns. Whether the threat of de-listing Chinese firms materializes will depend in part on how the Act is implemented by the U.S. Securities and Exchange Commission. However, the measure's approval by Congress without a single dissenting vote suggests that there is likely to be continuing support among U.S. policymakers for limiting Beijing's access to U.S. investors and capital.

D. Promoting Human Rights in Hong Kong

In connection with China's crackdown on protests in Hong Kong and the June 2020 enactment of China's new Hong Kong national security law—which criminalizes dissent through vague offenses such as secession, subversion, terrorism, and collusion with a foreign power—the United States moved to impose consequences on Beijing for undermining freedoms enshrined in the 1984 Sino-British Joint Declaration and Hong Kong's Basic Law. However, such U.S. measures have so far been limited in scope and have principally involved revoking Hong Kong's special trading status and imposing sanctions on several senior Hong Kong and mainland Chinese government officials. No governmental entity within the Special Administrative Region ("SAR") of Hong Kong has yet been sanctioned.

Under U.S. law, the Secretary of State must periodically certify that Hong Kong retains a "high degree of autonomy" from mainland China in order for the territory to continue receiving preferential treatment—including lower tariffs, looser export controls, and relaxed visa requirements—compared to the rest of China. On May 28, 2020, Secretary of State Mike Pompeo reported to the U.S. Congress that Hong Kong is no longer sufficiently autonomous to warrant such preferential treatment. Shortly thereafter, President Trump on July 14, 2020 issued Executive Order 13936 formally revoking Hong Kong's special trading status and signed into law the Hong Kong Autonomy Act ("HKAA"), which authorizes the President to impose sanctions such as asset freezes and visa bans on individuals and entities that enforce the new Hong Kong national security law. The HKAA also authorizes "secondary" sanctions on non-U.S. financial institutions that knowingly conduct significant transactions with persons that enforce the Hong Kong national security law—potentially subjecting non-U.S. banks that engage in such dealings to a range of consequences, including loss of access to the U.S. financial system.

With that policy framework in place, various arms of the U.S. government soon implemented more targeted measures designed to hold Hong Kong's leadership accountable and to conform Hong Kong's legal status with the rest of China.

Notably, on August 7, 2020, OFAC designated to the SDN List 11 senior Hong Kong and mainland Chinese government officials—including Hong Kong's chief executive, Carrie Lam—for their involvement in implementing the national security law. As a result of this action, U.S. persons (as well as non-U.S. persons when engaging in a transaction with a U.S. touchpoint) are, except as authorized by OFAC, generally prohibited from engaging in transactions involving these 11 individuals and their property and interests in property. Although OFAC has clarified in published guidance that the prohibition does not extend to routine dealings with the non-sanctioned government agencies that these individuals lead, U.S. persons should take care not to enter into contracts signed by, or negotiate with, government officials who are SDNs, activities which could trigger U.S. sanctions.

Meanwhile, the U.S. Department of Commerce in June 2020 suspended the availability of certain export license exceptions that treated Hong Kong more favorably than mainland China. As a result of this suspension—which appears to have been driven by concerns among U.S. policymakers that sensitive goods, software, and technology exported to Hong Kong could be diverted to the mainland—exports, reexports, or transfers to or within Hong Kong of items subject to the EAR may now require a specific license from the U.S. government. Further cementing this shift in U.S. policy, the U.S. Department of Commerce in December 2020 removed Hong Kong as a separate destination on the Commerce Country Chart, effectively ending Hong Kong's preferential treatment for purposes of U.S. export controls.

While the implementation of tougher sanctions and export controls represents an escalation of U.S. pressure on the Chinese government, the Trump administration during its final year in office shied away from imposing more draconian measures with respect to Hong Kong. For example, the United States has to date refrained from targeting non-U.S. banks, the Hong Kong SAR government, or acted to undermine the longstanding peg that has linked the Hong Kong Dollar and the U.S. Dollar—likely out of concern for the heavy collateral consequences that such measures could inflict on Hong Kong's pro-Western population, as well as on the many U.S. and multinational firms with operations in the city.

In our assessment, such severe measures—which could undermine Hong Kong's historic role as a global financial hub—are unlikely to be imposed by the Biden-Harris administration absent significant further deterioration in relations between Washington and Beijing. Instead, particularly in light of reports of a wave of arrests in January 2021 pursuant to the Hong Kong national security law, the Biden-Harris administration could designate additional Chinese and Hong Kong government officials for their role in eroding Hong Kong's autonomy. A further option available to President Biden could involve easing the path for Hong Kong residents to immigrate to the United States (in line with similar proposals mooted by the U.K. government)—which would both shield such individuals from repression and impose costs on Beijing by draining away some of Hong Kong's considerable human capital.

E. Promoting Human Rights in Xinjiang

During 2020, the United States ramped up legislative and regulatory efforts to address and punish reported human rights abuses in China's Xinjiang Uyghur Autonomous Region ("Xinjiang"). Although concerns about high-tech surveillance and harsh security measures against Muslim minority groups date back over a decade, the latest reports estimate that up to 1.5 million Uyghurs, Kazakhs, and other Turkic minorities have been detained in "reeducation camps" and that many others, including former detainees, have been forced into involuntary labor in textile, apparel, and other labor-intensive industries.

In response to these developments, President Trump on June 17, 2020 signed into law the

Uyghur Human Rights Policy Act of 2020. The Act required the President to submit within 180 days a report to Congress—which as of this writing has yet to be issued—that identifies foreign persons, including Chinese government officials, who are responsible for flagrant human rights violations in Xinjiang. The Act authorizes the President to impose sanctions (including asset freezes and visa bans) on persons identified therein, and directs the Department of State, the Director of National Intelligence, and the Federal Bureau of Investigation to submit reports to Congress on human rights abuses, and the national security and economic implications of the PRC's actions, in Xinjiang.

The Trump administration also took a number of executive actions against Chinese individuals and entities implicated in the alleged Xinjiang repression campaign. On July 9, 2020, OFAC designated to the SDN List the Xinjiang Public Security Bureau and four current or former Chinese government officials for their ties to mass detention programs and other abuses. On July 31, 2020, OFAC followed up on this action by sanctioning the Xinjiang Production and Construction Corps ("XPCC")—a state-owned paramilitary organization and one of the region's most economically consequential actors—plus two further government officials.

In tandem with sanctions designations, the United States during 2020 leveraged export controls to advance the U.S. policy interest in curtailing human rights abuses in Xinjiang—most notably through expanded use of the Entity List. As discussed in our 2020 Mid-Year Sanctions and Export Controls Update, BIS has over the past year continued to use its powerful Entity List designation tool to effectively ban U.S. exports to entities implicated by the interagency End-User Review Committee ("ERC") in certain human rights violations.

While the ERC has long had the power to designate companies and other organizations for acting contrary to U.S. national security and foreign policy interests, these interests historically have been focused on regional stability, counterproliferation, and anti-terrorism concerns, plus violations of U.S. sanctions and export controls. Beginning in October 2019, however, the ERC added human rights to this list of concerns, focusing especially on human rights violations occurring in Xinjiang and directed against Uyghurs, Kazakhs, and other members of Muslim minority groups in China. Accelerating this trend, the ERC on three separate occasions this past year—including in June, July, and December 2020—added a total of 24 Chinese organizations to the Entity List for their conduct in Xinjiang. Among the entities targeted were Chinese firms that enable high-tech repression by producing video surveillance equipment and facial recognition software, as well as Chinese companies that benefit from forced labor in Xinjiang such as manufacturers of textiles and electronic components. In addition to denying these entities access to controlled U.S.-origin items, these designations also spotlight sectors of the Chinese economy that are likely to remain subject to regulatory scrutiny under the Biden-Harris administration and which may call for enhanced due diligence by U.S. companies that continue to engage with Xinjiang.

Consistent with the Trump administration's whole-of-government approach to trade with China, the United States also used import restrictions—including a record number of withhold release orders issued by U.S. Customs and Border Protection ("CBP")—to deny certain goods produced in Xinjiang access to the U.S. market.

CBP is authorized to enforce Section 307 of the Tariff Act of 1930, which prohibits the importation of foreign goods produced with forced or child labor. Upon determining that there is information that reasonably, but not conclusively, indicates that goods that are being, or are likely to be, imported into the United States may be produced with forced or child labor, CBP may issue a withhold release order, which requires the detention of such goods at any U.S. port. Historically, this policy tool was seldom used until the latter half of the Obama administration.

During 2020, CBP ramped up its use of this policy instrument, issuing 15 withhold release orders—the most in any single year for at least half a century. Of those orders, nine were

focused on Xinjiang, including import restrictions on hair products and garments produced by certain manufacturers, as well as cotton and cotton products produced by XPCC, the Chinese paramilitary organization sanctioned by OFAC. On January 13, 2021, the Trump administration went further and imposed a withhold release order targeting all cotton products and tomato products originating from Xinjiang. Taken together, these developments suggest that the U.S. government is likely to continue its aggressive use of import restrictions against goods sourced from Xinjiang, further heightening the need for importers to scrutinize suppliers with ties to the region in order to minimize the risk of supply chain disruptions and reputational harm.

As a complement to the regulatory changes described above, the Trump administration during 2020 published multiple rounds of guidance to assist the business community in conducting human rights diligence related to Xinjiang. On July 1, 2020, the U.S. Departments of State, Treasury, Commerce, and Homeland Security issued the Xinjiang Supply Chain Business Advisory, a detailed guidance document for industry spotlighting risks related to doing business with or connected to forced labor practices in Xinjiang and elsewhere in China. The Advisory underscores that businesses and individuals engaged in certain industries may face reputational or legal risks if their activities involve support for or acquisition of goods from commercial or governmental actors involved in illicit labor practices and identifies potential indicators of forced labor, including factories located within or near known internment camps.

Separately, and as discussed further below, the U.S. Department of State on September 30, 2020 issued guidance specifically focused on exports to foreign government end-users of products or services with surveillance capabilities with an eye toward preventing such items from being used to commit human rights abuses of the sort reported in Xinjiang.

Underscoring the extent of U.S. concern about the situation in Xinjiang, then-Secretary of State Pompeo on the Trump administration's last full day in office issued a determination that the Chinese government's activities in the region constitute genocide and crimes against humanity—a declaration that was quickly echoed by current Secretary of State Antony Blinken in his Senate confirmation hearing. While the declaration triggers few immediate consequences under U.S. law, it could portend further U.S. sanctions designations related to China's treatment of ethnic and religious minorities.

F. Trade Imbalances and Tariffs

Also in 2020, the Trump administration continued to make broad use of its authority to impose tariffs on Chinese-made goods. This policy approach met with significant opposition from private plaintiffs, setting the stage for substantial and largely unresolved litigation at the U.S. Court of International Trade. The year began with significant tariffs already in place through two mechanisms: Section 232 of the Trade Expansion Act of 1962 ("Section 232"), which allows the President to adjust the imports of an article upon the determination of the U.S. Secretary of Commerce that the article is being imported into the United States in such quantities or under such circumstances as to impair the national security, and Section 301 of the Trade Act of 1974 ("Section 301"), which allows the President to direct the U.S. Trade Representative to take all "appropriate and feasible action within the power of the President" to eliminate unfair trade practices or policies by a foreign country.

1. Section 232

On January 24, 2020, President Trump issued a proclamation under Section 232 expanding the scope of existing steel and aluminum tariffs (25 percent and 10 percent, respectively) to cover certain derivatives of aluminum and steel such as nails, wire, and staples, which went into effect on February 8, 2020. President Biden has stated that he plans to review the Section 232 tariffs, although no immediate timetable for that review has

been set forth to date.

Two cases of note regarding the scope of the President's power to impose Section 232 tariffs were decided this year. In *Transpacific Steel LLC v. United States*, 466 F.Supp. 3d 1246 (CIT 2020), the court held that Proclamation 9772, which imposed a 50 percent tariff on steel products from Turkey, was unlawful because it violated Section 232's statutory procedures and the Fifth Amendment's Equal Protection guarantees. The court noted that Section 232 "grants the President great, but not unfettered, discretion," and agreed with the importers that the President acted outside the 90-day statutorily mandated window and without a proper report on the national security threat posed by steel imports from Turkey. The court also agreed that Proclamation 9772 denied the importers the equal protection of law because it arbitrarily and irrationally doubled the tariff rate on Turkish steel products and there was "no apparent reason to treat importers of Turkish steel products differently from importers of steel products from any other country listed in the" relevant report. While *Transpacific* limited the President's power to impose Section 232 tariffs, on February 28, 2020, the Federal Circuit rejected a constitutional challenge to Section 232 itself and held that Section 232 did not unlawfully cede authority to control trade to the President in violation of the Constitution's nondelegation doctrine, and the 232 tariffs remain in place.

On December 14, 2020, the Commerce Department published a notice announcing changes to the Section 232 steel and aluminum tariffs exclusions process. Changes include (1) the adoption of General Approved Exclusions for specific products; (2) a new volume certification requirement meant to limit requests for more volume than needed compared to past usage; and (3) a streamlined review process for "No Objection" exclusion requests.

2. Section 301

Although the Trump administration initiated Section 301 tariff investigations involving multiple jurisdictions, the Section 301 tariffs that have dominated the headlines are the tariffs imposed on China in retaliation for practices with respect to technology transfer, intellectual property, and innovation that the Office of the U.S. Trade Representative ("USTR") has determined to be unfair ("China 301 Tariffs"). The China 301 Tariffs were imposed in a series of waves in 2018 and 2019, and as originally implemented they together cover over $500 billion in products from China.

On January 15, 2020, the United States and China signed a Phase One Trade Agreement, leading to a slight reprieve in the U.S.-China trade dispute. As part of that agreement, the United States agreed to suspend indefinitely its List 4B tariffs and to reduce its List 4A tariffs to 7.5 percent. Pursuant to the agreement, China committed (1) to purchase an additional $200 billion in U.S. manufactured, agriculture, and energy goods and services as compared to a 2017 baseline; (2) to address U.S. complaints about intellectual property practices by providing stronger Chinese legal protections and eliminating pressure for foreign companies to transfer technology to Chinese firms as a condition of market access; (3) to implement certain regulatory measures to clear the way for more U.S. food and agricultural exports to China; and (4) to improve access to China's financial services market for U.S. companies. A "Phase Two" trade deal never materialized following strained relations between the two countries catalyzed in part over the coronavirus pandemic.

As the statute of limitations to challenge two of the larger China 301 Tariff tranches (List 3 and List 4A) approached with no further progress beyond the Phase One Trade Agreement, in an unprecedented act thousands of parties affected by the tariffs filed suit at the Court of International Trade, alleging that the tariffs were not properly authorized by the Trade Act of 1974, and that USTR violated the Administrative Procedure Act when it imposed them. More than 3,500 actions, some filed jointly by multiple plaintiffs, were filed, and case management issues are still under development: the U.S. Court of International

Trade has not yet designated a "test" case or cases—the case(s) which will be resolved first, while the rest of the cases are stayed pending resolution—or determined if the case(s) will be heard by a three-judge panel. These arguments are playing out on the docket of *HMTX Industries LLC v. United States*, Ct. No. 20-00177, which we presume will be a lead case.

Although the China 301 Tariffs were a hallmark of the Trump administration's trade policy, we expect them to remain in place under the Biden-Harris administration, at least during an initial period of review. President Biden has nominated Katherine Tai, the former lead trade attorney for the U.S. House of Representatives Ways and Means Committee, to serve as USTR. Her background includes significant China-related expertise—including successful litigation at the World Trade Organization, involvement in drafting proposed legislation on China-related issues, such as Uyghur forced labor, and experience as USTR's chief counsel for China enforcement—suggesting that China will remain a focus of U.S. trade policy going forward.

G. China's Counter-Sanctions – The Chinese Blocking Statute

The Chinese Blocking Statute, which we discuss at greater depth in our recent client alert, creates a reporting obligation for Chinese persons and entities impacted by extra-territorial foreign regulations. Critically, this reporting obligation is applicable to Chinese subsidiaries of multinational companies. The Chinese Blocking Statute also creates a private right of action for Chinese persons or entities to seek civil remedies in Chinese courts from anyone who complies with prohibited extra-territorial measures.

While the Chinese regulations remain nascent and the initial list of extra-territorial measures that the Chinese Blocking Statute will cover has yet to be published, the law marks a material escalation in the longstanding Chinese threats to impose counter-measures against the United States (principally) by establishing a meaningful Chinese legal regime that could challenge foreign companies with operations in China. If the European model for the Chinese Blocking Statute continues to serve as Beijing's inspiration, we will likely see both administrative actions to enforce the measure as well as private sector suits to compel companies to comply with contractual obligations, even if doing so is in violation of their own domestic laws.

The question for the United States with respect to this new Chinese law will be how to balance the aggressive suite of U.S. sanctions and export control measures levied against China—which the U.S. government is unlikely to pare back—against the growing regulatory risk for global firms in China that could be caught between inconsistent compliance obligations. As has long been the case, international companies will continue to be on the front lines of Washington-Beijing tensions and they will need to remain flexible in order to respond to a fluid regulatory environment and maintain access to the world's two largest economies.

H. New Chinese Export Control Regime

On December 1, 2020, the Export Control Law of the People's Republic of China ("China's Export Control Law") officially took effect. This marks a milestone on China's long-running efforts towards a comprehensive and unified export control regime and to large parts has been discussed in detail in our recent client alert.

By passing China's Export Control Law, China has formally introduced concepts common to other jurisdictions, yet new to China's export control regime such as, inter alia, embargos, into its export control regime, and particularly expands the scope of China's Export Control Law to have an extraterritorial effect. Compared to China's prior export control rules scattered in various other laws and regulations, China's Export Control Law has also imposed significantly enhanced penalties in case of violations. Pursuant to

China's Export Control Law, the maximum monetary penalties in certain violations could reach 20 times the illegal income. Any foreign perpetrators may also be held liable, although unclear how.

Before this new law came into effect, China already took actions to curb the export control of sensitive technologies. On August 28, 2020, in the midst of the forced TikTok sale demanded by the U.S. government, China amended its Catalogue of Technologies Whose Exports Are Prohibited or Restricted to capture additional technologies, including "personalized information push service technology based on data analysis" that is relied upon by TikTok. Such inclusion would make it extremely challenging, if not impossible, to export the captured technologies because "substantial negotiation" of any technology export agreement with respect to such technology may not be conducted without the approval of the relevant Chinese authorities.

In addition to China's Export Control Law, detailed provisions with respect to China's unreliable entity list were unveiled on September 19, 2020, namely, the Provisions on the Unreliable Entities List. This unreliable entity list, which may include foreign companies and individuals (although none has been identified so far), has been deemed by some as China's attempt to directly counter BIS's frequent use of its entity list. For those listed in China's unreliable entity list, China-related import and export, investment and other business activities may be restricted or prohibited.

Although there has been no official update so far with respect to exactly whom or which entity would be placed on China's control list or unreliable entity list, China has imposed sanctions on a number of U.S. individuals and entities in the second half of 2020, which has been perceived as a counter measure against U.S.'s sanctions of Chinese (including Hong Kong) entities and officials.

For instance, on December 10, 2020, shortly after the Hong Kong-related designations by the U.S. Department of the Treasury on December 7, 2020, a spokesperson from China's Ministry of Foreign Affairs announced sanctions against certain U.S. officials for "bad behavior" over Hong Kong issues and revoked visa-free entry policy previously granted to U.S. diplomatic passport holders when visiting Hong Kong and Macau.

II. U.S. Sanctions Program Developments

A. Iran

During the second half of 2020, the outgoing Trump administration and then-candidate Biden articulated sharply contrasting positions on Iran sanctions—both bearing the hallmarks of their broader approaches to foreign policy. In its final push for "maximum economic pressure," the Trump administration sought to impose additional sanctions that would make it more difficult for the Biden-Harris administration to reenter the JCPOA, the nuclear deal negotiated by the Obama administration. At the same time, then-candidate Biden laid out his plan to reengage with Iran, reinstate compliance with the JCPOA, and roll back the U.S. sanctions that had been re-imposed.

With the international community rebuffing efforts to abandon the JCPOA and Iran's current government signaling interest in a quick return to the deal, the stage could be set for the Biden-Harris administration to achieve its goals for Iran, although the timing is uncertain. Domestic political concerns in both countries, a global pandemic, and pressure from U.S. allies in the Middle East could frustrate these efforts and ensure the sanctions

status quo remains in the near term.

The Trump administration's effort in August and September to snap United Nations sanctions back into effect marked the culmination of a years-long campaign intended to drive Iran to negotiate a more comprehensive deal for relief. Where the JCPOA only addressed Iran's nuclear program, the Trump administration sought an agreement regulating more facets of Iran's "malign activities" in return for sanctions relief. The "maximum economic pressure" campaign began in earnest in November 2018 with the full re-imposition of sanctions that had been lifted under the terms of the JCPOA. As we discussed in our 2019 Year-End Sanctions Update, the campaign continued throughout 2019, as the United States targeted new industries and entities and ramped up pressure on previously sanctioned persons.

The Trump administration continued increasing this pressure over the course of 2020, while clarifying the scope of humanitarian exemptions in response to the global coronavirus pandemic. Our 2020 Mid-Year Sanctions and Export Controls Update details re-imposition of restrictions on certain nuclear activities, a steady stream of new designations, and the expansion of U.S. secondary sanctions to target new sectors of the Iranian economy. This increasing pressure was accompanied by several measures designed to facilitate Iran's response to the coronavirus pandemic, including additional interpretive guidance, approved payment mechanisms, and a new general license.

Trump administration efforts in the latter half of 2020 were more focused on maximizing economic pressure on Iran. OFAC made use of new secondary sanctions authorities to impose additional sanctions on Iran's financial sector, and announced further authorities targeting conventional arms sales to Iran, responding directly to the impending rollback of UN sanctions. The steady stream of designations also continued, with OFAC focusing particularly on entities operating in or supporting Iran's petroleum and petrochemicals trade (see e.g., designation announcements in September, October, and December), including additional restrictions on the Iranian Ministry of Petroleum, the National Iranian Oil Company ("NIOC"), and the National Iranian Tanker Company ("NITC"). OFAC also designated several rounds of new targets, including senior officials in the Iranian government, for alleged involvement in human rights violations.

Despite this mounting economic pressure, Iran has still found ways to slip through the grasp of the tightening embargo. In the fall of 2020, market watchers observed a sharp uptick in Iranian oil exports. Increasing demand among U.S. adversaries—including China and Venezuela—along with steep discounts from Iran have likely contributed to the spike in exports. Increasingly-sophisticated evasion tactics have helped too—despite State Department guidance published in May 2020 to address these deceptive shipping practices.

The U.S. also continued to pursue criminal penalties for entities that tried to evade U.S. sanctions. In August, the United States charged an Emirati entity and its managing director for implementing a scheme to circumvent U.S. sanctions and supply aircraft parts to Mahan Air, an Iranian airline and longtime target of U.S. export controls and sanctions designated for supporting Iran's Islamic Revolutionary Guard Corps' Quds Force. OFAC simultaneously imposed sanctions on those Emirati targets, as well as several other associated entities. These enforcement efforts hit one notable setback in July, when a judge in the Southern District of New York dismissed a case against Ali Sadr Hashemi Nejad, who had been convicted of using the U.S. financial system to process payments to Iran. The judge vacated Mr. Nejad's conviction after the U.S. Attorney's office revealed alleged misconduct by the prosecutors that originally tried the case—including efforts to "bury" evidence turned over to the defense.

Efforts to increase pressure on Iran reached their zenith with the Trump administration's unilateral push to trigger the snapback of broad international sanctions on Iran. In an effort to ensure that the JCPOA remained responsive to concerns about Iran's compliance, the original parties included a mechanism that would allow the UN-based

international sanctions regime to snap back into place if a party to the agreement brought a compliant that Iran was not in compliance. The United States attempted to trigger this snapback mechanism by submitting allegations of Iranian noncompliance to the UN Security Council on August 20, 2020. The other members of the Security Council flatly rejected the U.S. efforts. They argued that the United States, which had withdrawn from the agreement in 2018, no longer had standing to trigger the snapback, and, although they acknowledged Iran's noncompliance, they expressed a preference for resolving the issue within the confines of the JCPOA. Nevertheless, in keeping with the timelines provided in the JCPOA, Secretary Pompeo announced "the return of virtually all previously terminated UN sanctions" on September 19. The remaining members of the JCPOA ignored the announcement and did not re-impose restrictions.

This fatigue with the current U.S. position and the calls for further leniency in response to the pandemic have created an international environment that may facilitate the Biden-Harris administration's plans to return to the JCPOA. President Biden and his National Security Adviser, Jake Sullivan, have clearly stated that, if Iran returns to "strict compliance," the administration would rejoin the JCPOA. For its part, Iranian President Hassan Rouhani has announced that Iran would hasten to comply with the JCPOA if the U.S. were to rejoin. Iran's supreme leader, Ayatollah Ali Khamenei, may also favor a return to the JCPOA, as more reliable oil revenues are important to help ensure future domestic stability.

However, the window for a return to the JCPOA may be narrow and may not accommodate the Biden-Harris administration's desire for follow-on agreements addressing other aspects of Iran's malign activities. Iranian elections are coming up in June, and hard-liners have signaled their opposition to a revived JCPOA. Iran has also increased its uranium enrichment and begun construction projects at its most significant nuclear facilities. This activity could embolden domestic opposition in the United States, where there is already limited appetite for a return to the basic JCPOA structure. Even close Biden ally Senator Chris Coons (D-DE) has suggested that a revised deal should address not only the nuclear issues covered by the JCPOA but also Iran's missile program. If domestic political concerns prevent a return to the agreement, sanctions could continue to tighten and could even return to pre-JCPOA levels if Iran intensifies its noncompliance.

B. Venezuela

Despite the far reaching effects of OFAC's current Venezuela sanctions program, which has crippled Venezuela's state-owned oil company, Petróleos de Venezuela, S.A. ("PdVSA"), the regime of President Nicolás Maduro remains firmly entrenched, and emerged victorious from a December 2020 legislative election that U.S. Secretary of State Mike Pompeo described as a "political farce." The results have made it increasingly difficult for Venezuela's opposition movement seeking to oust Maduro, further undermining opposition leader and Interim President Juan Guaidó. The economic devastation, political instability, and compounding impacts of the pandemic have continued the refugee crisis pressuring some of Venezuela's neighbors and creating an even more delicate security environment for the Biden-Harris administration.

At the end of 2020, Biden-Harris transition representatives suggested that the new administration would push for free and fair elections in Venezuela in exchange for sanctions relief, but not necessarily to require Maduro's surrender as a condition of negotiations. The approach is expected to be coordinated with international allies, and Maduro's foreign backers in Russia, China, Iran and Cuba will likely be involved. The Biden-Harris team has promised to review existing OFAC sanctions with respect to Venezuela, assessing which potential measures may be lifted as part of any future discussions.

As we described in our 2020 Mid-Year Sanctions and Export Controls Update, last year

the Trump administration 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 with sanctions, including designating prominent Chinese and Russian companies involved with the sector. 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 sell off the relevant assets and operations to a unnamed company. On November 30, 2020, OFAC announced another major designation under the Venezuela sanctions program, ***China National Electronic Import-Export Company ("CEIEC")***. OFAC explained that CEIEC supported the Maduro regime's "malicious cyber efforts," including online censorship, strategically timed intentional electricity and cellphone blackouts, and a fake website purportedly for volunteers to participate in the delivery of international humanitarian aid that was actually designed to phish for personal information. CEIEC has over 200 subsidiaries and offices worldwide, and through the application of OFAC's 50 Percent rule any subsidiaries that are at least half-owned by CEIEC will be subject to the same restrictions as CEIEC.

On December 18, 2020, OFAC designated a Venezuelan entity and two individuals for providing material support to the Maduro regime, including by providing goods and services used to carry out the "fraudulent" parliamentary elections. On December 30, 2020, OFAC designated a Venezuelan judge and prosecutor for involvement in the unfair trial of the "Citgo 6," six executives of PdVSA's U.S. subsidiary Citgo who were lured to Venezuela under false pretenses and arrested in 2017.

OFAC also narrowed the scope of activities authorized by several general licenses. 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 PdVSA. On November 17, 2020, OFAC extended this narrowed version of General License 8 through June 3, 2021. On January 4, 2021, OFAC revised General License 31A , which authorized certain transactions involving the Venezuelan National Assembly and Guaidó, to specify that it applies only to the members of the National Assembly seated on January 5, 2016, *i.e.* prior to the December 2020 election.

C. Cuba

The Trump administration continued its pressure on Cuba in 2020, in an ostensible attempt to appeal to Cuban-American and other voters in Florida prior to the election and then to bind the incoming Biden-Harris administration from shifting course in U.S.-Cuba relations. The new U.S. administration had previously nodded to changes in U.S.-Cuba relations, with then-candidate Biden criticizing the Trump administration for inflicting harm on the Cuban people and promising to roll back certain Trump's policies. That said, Biden-Harris representatives acknowledged that significant change was unlikely to happen anytime soon.

1. Designations and Remittance Restrictions

As we analyzed in our 2020 Mid-Year Sanctions and Export Controls Update, the Trump administration added numerous entities to the State Department's Cuba Restricted List this year, thus prohibiting U.S. persons and entities from engaging in direct financial transactions with them and imposing certain U.S. export control licensing requirements. Between June and September 2020, the State Department added numerous Cuban military-owned sub-entities—most operating in Cuba's tourism industry—to the Cuba Restricted List, including the financial services company ***Financiera Cimex ("FINCIMEX")*** and its subsidiary ***American International Services ("AIS")***. In October 2020, OFAC amended the Cuban Assets Control Regulations ("CACR") to prohibit indirect remittance transactions with entities on the Cuba Restricted List, including transactions relating to the collection, forwarding, or receipt of remittances. The U.S. administration turned the screws again on FINCIMEX in December 2020, designating it, ***Kave Coffee***, and their

Cuban military-controlled umbrella enterprise ***Grupo de Administración Empresarial ("GAESA")*** to the SDN List. On January 15, 2021, five days before President Biden's inauguration, OFAC designated the Cuban Ministry of Interior ("MININT") and its leader, Lazaro Alberto Álvarez Casas, for human rights abuses relating to the monitoring of political activity. According to OFAC, Cuban dissident Jose Daniel Ferrer was beaten, tortured, and held in isolation in a MININT-controlled prison in September 2019.

2. State Sponsor of Terrorism Determination

Furthermore, on January 11, 2021, the State Department re-designated Cuba as a State Sponsor of Terrorism ("SST"), on the grounds that Cuba "repeatedly provid[es] support for acts of international terrorism in granting safe harbor to terrorists," and in a direct reversal of a May 2015 decision by the Obama administration to remove that designation. An SST designation imposes several restrictions, including a ban on Cuba-related defense exports, credits, guarantees, other financial assistance, and export licensing overseen by the State Department (Section 40 of the Arms Export Control Act); a license requirement (with a presumption of denial) for exports of dual-use items to Cuba (Section 1754(c) of the National Defense Authorization Act for Fiscal Year 2019); and a ban on U.S. foreign assistance to Cuba (Section 620A of the Foreign Assistance Act). The SST designation opens the door for other U.S. federal agencies to impose further restrictions, and it remains to be seen how the new Biden-Harris administration will navigate the course. When President Obama lifted the designation, that procedure required months of review by the State Department, a 45-day pre-notification period for Congress, and a cooperative Congress that did not exercise the blocking authority made available to it under the Arms Export Control Act.

3. Travel Restrictions

In September 2020, OFAC amended the CACR for the first time since September 2019. In this amendment, OFAC targeted Cuba's travel, alcohol, and tobacco industries by prohibiting any U.S. person from engaging in lodging transactions, either directly or indirectly, with any property that the Secretary of State has identified as owned or controlled by the Cuban government or its prohibited officials and their relatives. Concurrent with this change, the State Department published the new Cuba Prohibited Accommodations List to identify the lodging properties that would trigger this prohibition. Additionally, the CACR amendment eliminated certain general licenses to restrict attendance at professional meetings or conferences in Cuba and attendance at or transactions incident to public performances, clinics, workshops, other athletic or non-athletic competitions, and exhibitions in Cuba.

4. Helms-Burton Act

As we wrote in May 2019, on April 17, 2019, the Trump administration lifted long-standing limitations on American citizens seeking to sue over property confiscated by the Cuban regime after the revolution led by Fidel Castro six decades ago. Title III of the Cuban Liberty and Democratic Solidarity ("LIBERTAD") Act of 1996, commonly known as the Helms-Burton Act, authorizes current U.S. citizens and companies whose property was confiscated by the Cuban government on or after January 1, 1959 to bring suit for monetary damages against individuals or entities that "traffic" in that property. The policy rationale for this private right of action was to provide recourse for individuals whose property was seized by the Castro regime. As part of the statutory scheme, Congress provided that the President may suspend this private right of action for up to six months at a time, renewable indefinitely. Until May 2019, U.S. Presidents of both parties had consistently suspended that statutory provision in full every six months. While President Biden could suspend the private right of action, already-existing Title III lawsuits are authorized under the Helms-Burton Act to run to completion, inclusive of any appeals.

D. Russia

Although the COVID-19 pandemic and resulting economic crisis dominated President Biden's first few days in office, his administration was forced to act fast to achieve an extension of the New Strategic Arms Reduction Treaty ("New START") arms control treaty ahead of a February 5, 2021 deadline. The extension to February 4, 2026, does not necessarily portend any greater degree of cooperation between the two countries, however, as the new U.S. administration has suggested that it may impose new measures on Russia pending an intelligence assessment of its recent activities.

1. CAATSA Section 224 Russian Cyber Sanctions

As noted above, U.S. federal agencies are still assessing the scope and impact of the recent Russian cyberattack that breached network security measures of at least half a dozen cabinet-level agencies and many more private sector entities, which could lead to sanctions under a 2015 Executive Order targeting persons engaged in malicious cyber activities or Section 224 of the Countering America's Adversaries Through Sanctions Act ("CAATSA"). There is recent precedent for such actions—on October 23, 2020, OFAC designated Russia's State Research Center of the Russian Federation FGUP Central Scientific Research Institute of Chemistry and Mechanics ("TsNIIKhM") pursuant to Section 224 of CAATSA for TsNIIKhM's involvement in the development and spread of Triton malware, also known as TRISIS or HatMan, which targets and manipulates industrial safety systems and has been described as "the most dangerous" publicly known cybersecurity threat. Triton first made news in 2017 after it crippled a petrochemical plant in Saudi Arabia, and OFAC warned that Russian hackers had turned their attention to U.S. infrastructure, where at least 20 electric utilities have been probed by hackers for vulnerabilities since 2019.

2. CAATSA Section 231 Russian Military Sanctions

On December 14, 2020, the United States imposed sanctions on the Republic of Turkey's Presidency of Defense Industries ("SSB"), the country's defense procurement agency, and four senior officials at the agency, for its dealings with Rosoboronexport ("ROE"), Russia's main arms export entity, in procuring the S-400 surface-to-air missile system. As we described in December 2020, Section 231 of CAATSA required the imposition of sanctions on any person determined to have knowingly engaged in a significant transaction with the defense or intelligence sectors of the Russian government. Notwithstanding Section 231's mandatory sanctions requirement, the Trump administration repeatedly tried to pressure Turkey to abandon the ROE deal before sanctions were imposed. In line with a growing list of non-SDN measures managed by OFAC (including the Sectoral Sanctions and the Communist Chinese Military Companies investment restrictions), these sanctions are not full blocking measures and the SSB listing led OFAC to construct a new Non-SDN Menu-Based Sanctions List.

3. CAATSA Section 232 Nord Stream 2 and TurkStream Sanctions

U.S. efforts to block Russia's ongoing construction of major gas export pipelines to bypass Ukraine have been a longstanding source of tension not just between Washington and Moscow but also with the United States' core European allies. In Section 232 of CAATSA, Congress authorized—but did not require—the President to impose certain sanctions targeting Russian energy export pipelines "in coordination with allies of the United States," a statement of apparent deference to NATO allies like Germany and Turkey that would benefit most from the construction of the Nord Stream 2 and the TurkStream pipelines. That deference waned in the intervening years, and as we wrote in our 2019 Year-End Sanctions Update, the National Defense Authorization Act for Fiscal Year 2020 ("2020 NDAA") included provisions *requiring* the imposition of sanctions against

vessels and persons involved in the construction of the Nord Stream 2 and the TurkStream pipelines. Although the inclusion of these sanctions signaled U.S. support for Ukraine, their impact was thought to be minimal as the pipelines' construction was nearly complete (only one 50-mile gap remained of the Nord Stream 2 pipeline).

But the impact was more severe than anticipated. On July 15, 2020, the Department of State updated its guidance concerning the applicability of sanctions under Section 232 of CAATSA, expanding its scope to almost all entities involved in the construction of the Nord Stream 2 or TurkStream gas pipelines, not just to those who initiated their work after CAATSA's enactment. And on January 1, 2021, as part of the NDAA for Fiscal Year 2021, Congress amended CAATSA to authorize sanctions for foreign persons whom the Secretary of State, in consultation with the Secretary of the Treasury, deems to have knowingly helped provide pipe-laying vessels for Russian energy export pipelines.

Despite these sanctions—as well as growing domestic opposition to Russia in the aftermath of the poisoning of Russian opposition leader Aleksei Navalny—Germany remains committed to completing Nord Stream 2, which is now over 90 percent finished. Indeed, in early January, Germany's Mecklenburg-Vorpommern State Parliament voted to create a state-owned foundation to facilitate the pipeline's construction, taking advantage of an exemption added on January 1 for EU governmental entities not operating as a business enterprise.

4. Other Recent Russian Designations

In July 2020, OFAC targeted Russian financier Yevgeniy Prigozhin's wide-ranging network of companies in Sudan, Hong Kong and Thailand. Prigozhin has been the target of U.S. sanctions since 2016, and purportedly financed the Internet Research Agency, a Russian troll farm designated by OFAC in 2018, as well as Private Military Company ("PMC") Wagner, a Russian military proxy force active in Ukraine, Syria, Sudan and Libya that was designated by OFAC in 2017. OFAC highlighted Prigozhin's role in Sudan and the "interplay between Russia's paramilitary operations, support for preserving authoritarian regimes, and exploitation of natural resources." OFAC also targeted Prigozhin's network of financial facilitators in Hong Kong and Thailand. In September 2020, OFAC imposed sanctions on entities and individuals working on behalf of Prigozhin to advance Russia's interest in the Central African Republic ("CAR").

Also in September, OFAC imposed blocking sanctions on Andrii Derkach, a member of the Ukrainian parliament and an alleged agent of Russia's intelligence services. According to the U.S. Department of the Treasury, Derkach waged a "covert influence campaign" against then-candidate Biden by distributing false and unsubstantiated narratives through media outlets and social media platforms with the aim of undermining the 2020 U.S. presidential election. An additional round of sanctions was announced on January 11, targeting individuals and news outlets in Ukraine that cooperated with Derkach in his efforts to interfere in the 2020 U.S. election. OFAC also extended two Ukraine-related General Licenses, 13P and 15J, that permit U.S. persons to undertake certain transactions related to ***GAZ Group***, which was among the Russian entities designated on April 6, 2018 for being owned by one or more Russian oligarchs or senior Russian government officials. Among other actions, the regulatory authorizations, extended for over one year to January 26, 2022, allow U.S. persons to transfer or divest their holdings in GAZ Group to non-U.S. persons, allow U.S. persons to facilitate the transfer of holdings in GAZ Group by a non-U.S. person to another non-U.S. person, and allow U.S. persons to engage in certain transactions related to the manufacture and sale of automobiles, trucks, and other vehicles produced by GAZ Group or its subsidiaries.

E. North Korea

As we described in our 2020 Mid-Year Sanctions and Export Controls Update, the United States continued to expand its campaign to isolate North Korea economically and to cut off

illicit avenues of international support for its nuclear, chemical, and biological weapons programs. In addition to amending the North Korea Sanctions Regulations ("NKSR"), U.S. authorities issued sanctions advisories and pursued multiple enforcement actions against persons who violated these sanctions.

1. NKSR Amendments

On April 10, 2020, OFAC issued amendments to the NKSR, 31 C.F.R. part 510, to implement certain provisions of the North Korea Sanctions and Policy Enhancement Act of 2016 ("NKSPEA"), as amended by CAATSA, and the 2020 NDAA. Changes included implementing secondary sanctions for certain transactions; adding potential restrictions to the use of correspondent accounts for non-U.S. financial institutions that provide significant services to identified 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."

These amendments mark a significant jurisdictional expansion; in addition to potential secondary sanctions for foreign financial institutions that conduct significant business with North Korea, foreign banks that are subsidiaries of U.S. financial institutions are now directly subject to the NKSR. Thus, although the ailing condition of North Korea's economy may limit the impact of these measures on the international community, they put global financial institutions on notice to be vigilant with sanctions compliance and mindful of any dealings with North Korea.

2. Ballistic Missile Procurement Advisory

On September 1, 2020, the U.S. Departments of State, Treasury, and Commerce issued an advisory on North Korea's ballistic missile procurement activities. The advisory identified key North Korean procurement entities, including the Korea Mining Development Trading Corporation ("KOMID"), the Korea Tangun Trading Corporation ("Tangun"), and the Korea Ryonbong General Corporation ("Ryonbong"), and provided an annex identifying the main materials and equipment that North Korea is looking to source internationally for its ballistic missile program. The guidance also highlighted various procurement tactics that North Korea employs, including using North Korean officials accredited as diplomats to orchestrate the acquisition of sensitive technology; collaborating with foreign-incorporated companies (often Chinese and Russian entities) to acquire foreign-sourced basic commercial components; and mislabeling sensitive goods to escape export control requirements or to conceal the true end user.

The advisory emphasized that suppliers must not only watch for items listed in the Annex—or on U.S. or UN control lists—but also for widely available items that may end up contributing to the production or development of weapons of mass destruction ("WMD"). The electronics, chemical, metals, and materials industries, as well as the financial, transportation, and logistics sectors, are at particular risk of such end-use exposure and must pay heed to "catch-all" controls, such as United Nations Security Council Resolution ("UNSCR") 2270, that require authorization, like a license or permit, if there is any risk that their products may contribute to WMD-related programs. Consistent with OFAC's compliance framework, the advisory encouraged companies to take a risk-based approach to sanctions compliance.

3. SDN Designations in the Shipping Industry

In May 2020, OFAC, the Department of State, and the U.S. Coast Guard issued a global advisory warning the maritime industry, as well as the energy and metals sectors, about deceptive shipping practices used to evade sanctions. Numerous designations throughout the course of 2020 demonstrate OFAC's continued focus on the shipping industry and North Korean trade. On December 8, 2020, OFAC designated six entities and four

vessels for violating UNSCR 2371's restrictions on transporting or exporting North Korean coal. Designees include several Chinese entities (two of which were also registered in the United Kingdom), as well as companies in Hong Kong and Vietnam.

4. Criminal Enforcement

The violation of North Korean sanctions also continues to be an enforcement priority for both OFAC and U.S. Department of Justice. As we described in our 2020 Mid-Year Sanctions and Export Controls Update, on May 28, 2020, DOJ unsealed an indictment charging 33 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.

DOJ and OFAC have also focused on non-North Korean companies who have supported the efforts of their North Korean customers to access the U.S. financial system. In July 2020, OFAC and DOJ announced parallel resolutions with UAE-based ***Essentra FZE Company Limited ("Essentra")*** for violating the NKSR by exporting cigarette filters to North Korea using deceptive practices, including the use of front companies. On August 31, 2020, DOJ announced that ***Yang Ban Corporation ("Yang Ban")***, a company established in the British Virgin Islands that operated in South East Asia, pled guilty to conspiring to launder money in connection with evading sanctions on North Korea and deceiving correspondent banks into processing U.S. dollar transactions.

Lastly, on January 14, 2021, OFAC announced a settlement with Indonesian paper products manufacturer ***PT Bukit Muria Jaya ("BMJ")*** to resolve alleged violations of the NKSR connected to the exportation of cigarette paper to North Korea. DOJ announced a parallel resolution with BMJ through a Deferred Prosecution Agreement ("DPA") to resolve allegations of conspiracy to commit bank fraud shortly thereafter. The Yang Ban and BMJ matters highlight DOJ's increasing use of the money laundering and bank fraud statutes to pursue criminal cases related to sanctions violations, as neither case included an alleged violation of IEEPA.

F. Syria

OFAC continues to maintain a comprehensive and wide-ranging sanctions regime against the Bashal al-Assad regime in Syria. On August 20, 2020, OFAC designated Assad's press officer and the leader of the Syrian Ba'ath Party under Executive Order 13573 as senior Government of Syria officials, while the State Department simultaneously imposed sanctions on several individuals under Executive Order 13894 for their role in "the obstruction, disruption, or prevention of a political solution to the Syrian conflict and/or a ceasefire in Syria."

On September 30, 2020, OFAC and the State Department designated additional "key enablers of the Assad regime," including the head of the Syrian General Intelligence Directorate, the Governor of the Central Bank of Syria, and a prominent businessman (and his businesses) who served as a local intermediary for the Syrian Arab Army, while on November 9 OFAC and State designated additional individuals and entities, focusing on stymying Syria's attempt to revive its petroleum industry. Rounding out the year, on December 22, 2020, OFAC and the State Department sanctioned additional senior government officials and entities, including Assad's wife, Asma al-Assad—who had already been designated in June 2020—as well as several members of her family.

Additionally, on December 22, OFAC officially designated the Central Bank of Syria ("CBS") as an SDN. However, as the accompanying press release noted, the CBS has been blocked under Executive Order 13582 since 2011. As a simultaneously issued FAQ states, the designation "underscore[es] its blocked status" but "does not trigger new prohibitions." The FAQ includes the reminder that "non-U.S. persons who knowingly provide significant financial, material, or technological support to, or knowingly engage in a significant transaction with the Government of Syria, including the [CBS], or certain other

persons sanctioned with respect to Syria, risk exposure to sanctions." Another FAQ, issued on the same date, reiterated that U.S. and non-U.S. persons can continue engage with CBS in authorized transactions that provide humanitarian assistance to Syria, and clarified that OFAC will not consider transactions to be "significant" if they are otherwise authorized to U.S. persons, and therefore non-U.S. persons are not prohibited from participating in transactions that provide humanitarian assistance to the people of Syria.

G. Other Sanctions Developments

1. Belarus

During the second half of 2020, OFAC designated several individuals and entities for their role in participating in the fraudulent August 9, 2020 Belarus presidential election or the violent suppression of the peaceful protests that followed. Beginning in August 2020, the Belarusian government instituted a violent crackdown on wide scale protests that had erupted following the reelection of longtime leader Aleksandr Lukashenko, which had been widely denounced as fraudulent. The crackdown was broadly condemned internationally, with both the U.S. and EU imposing sanctions on those determined to have been involved in orchestrating the election fraud or the subsequent violence.

On October 2, 2020, OFAC, in coordination with the United Kingdom, Canada, and EU, designated eight individuals under Executive Order 13405, which was initially promulgated in response to Lukashenko's questionable reelection in 2006. The eight individuals include Belarus's Interior Minister and his deputy, the leaders of organizations involved in violently suppressing protesters, the Commander and Deputy Commander of the Ministry of the Interior's Internal Troops, and the Central Election Commission's Deputy Chairperson and Secretary. Several months later, on December 23, OFAC designated the Chief of the Criminal Police as well as four entities involved in the administration of the election and subsequent crackdown. The EU similarly imposed three rounds of sanctions on a total of 88 individuals and 7 entities following the August 9, 2020 election, while Canada and the United Kingdom also imposed sanctions on Belarus.

2. Ransomware Advisory

On October 1, 2020, OFAC issued an "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," which details the sanctions risk posed by paying ransom to malicious cyber actors on behalf of victims of cyberattacks. The Advisory provides several examples of SDNs who have been designated due to their malicious cyber activities, and underscores the prevalence of such actors on OFAC's sanctions lists. While the Advisory did not break new ground, it emphasizes that facilitating a ransomware payment, even on behalf of a victim of an attack, could constitute a sanctions violation, including in cases where a non-U.S. person causes a U.S. person to violate sanctions (in this case, to make the ransom payment to an SDN on behalf of the U.S. victim).

3. Art Advisory

One month later, on October 30, 2020, OFAC issued an "Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork." The Advisory underscores the sanctions risk posed by dealing in high value artwork—in particular artwork valued in excess of $100,000—due to the prevalence of SDNs' participation in the market. The Advisory details how SDNs take advantage of the anonymity and confidentiality characteristic of the market to evade sanctions and even provides several examples of SDNs—including a top Hizballah donor, two Russian oligarchs, and a sanctioned North Korean art studio—who have taken advantage of the high-end art market to evade sanctions.

The Advisory further encourages U.S. persons and companies, including galleries,

museums, private collectors, and art brokers, to implement risk-based compliance programs to mitigate against these risks. Further, and significantly, the Advisory clarifies that although the import and export of artwork is exempted from regulation under the Berman Amendment to IEEPA (which exempts from sanctions the export of information), OFAC does not interpret this exemption to encompass the intentional evasion of sanctions via the laundering of financial assets through the purchase and sale of high value artwork.

4. Hizballah Designations

OFAC has continued to put pressure on Hizballah through the imposition of sanctions in the second half 2020, particularly in the wake of the explosion at the Port of Beirut in August 2020, which highlighted the corruption and mismanagement that had become endemic to the Lebanese government. By the end of 2020, over 95 Hizballah-affiliated individuals and entities had been designated by OFAC since 2017. On September 8, 2020, OFAC designated two Lebanese government ministers for having "provided material support to Hizballah and engaged in corruption." Both ministers reportedly took bribes from Hizballah in return for granting the organization political and business favors. Fewer than two weeks later, on September 17, 2020, OFAC designated two Lebanese companies for being owned or controlled by Hizballah, as well as a senior Hizballah official, who is "closely associated" with the companies. The companies, which are controlled by Hizballah's Executive Council, reportedly had been used by Hizballah to evade sanctions and conceal the organization's funds. One month later, on October 22, 2020, OFAC designated two members of Hizballah's Central Council, which is the body that elects the organization's ruling Shura Council.

5. International Criminal Court-Related Designations

On September 2, 2020, the United States designated the chief prosecutor of the International Criminal Court ("ICC"), as well as an ICC senior official, to the SDN List, the first promulgation of sanctions pursuant to a June 11, 2020 Executive Order—which we discussed in more detail in our 2020 Mid-Year Sanctions and Export Controls Update—declaring the ICC to be a threat to the national security of the United States due to its ongoing investigation of U.S. military actions in Afghanistan.

On January 21, 2020, a court in the Southern District of New York issued a preliminary injunction against the government, enjoining it from enforcing aspects of the Executive Order and its implementing regulations (that had been published on September 30, 2020). In so doing, the court determined that, by preventing U.S. persons and organizations from providing advice or other speech-based support to the designated individuals, the restrictions infringe on the plaintiffs' constitutional right to free speech. Although the court has yet to issue a final ruling, the case may become mooted if the Biden-Harris administration revokes or allows the Executive Order to lapse, as commentators speculate.

III. U.S. Export Controls

Although China was often an explicit or implicit focus of many developments in U.S. export controls, 2020 was also year of significant innovation more broadly in export controls, especially those administered by the Department of Commerce. Each innovation has brought with it added complexities for compliance.

A. Commerce Department

1. Emerging Technology Controls

The Department of Commerce's Advanced Notice of Proposed Rule Making on Emerging Technologies in late 2018 sparked strong concern within many economic sectors that the Department was planning to swiftly act on its mandate under the Export Control Reform Act ("ECRA") of 2019 to identify and impose new and broadly framed controls concerning emerging technologies. However, as 2020 began—and even before the coronavirus took hold—it became clear that Commerce, for a few reasons, planned to take it slow**.** Commerce took well into late 2019 to analyze the public comments and to host many non-public meetings with a range of private sector actors, interagency, and non-government stakeholders on emerging technology controls. Among the key takeaways Commerce has shared publicly is its determination that emerging technology controls need to be tailored narrowly, and that Commerce needed to persuade other countries to adopt similar export controls to minimize the impact on the U.S. private sector companies and other organizations that are developing them.

The United States has several different ways to promote multilateral controls, including through its participation in the 42 member Wassenaar Arrangement ("WA"). Through its inter-plenary work in 2019, the participating states of the WA achieved consensus to impose new controls on six specific technologies at the December 2019 Wassenaar Arrangement Plenary, and in October 2020, Commerce added new controls on: hybrid additive manufacturing (AM)/computer numerically controlled ("CNC") tools; computational lithography software designed for the fabrication of extreme ultraviolet ("EUV") masks; technology for finishing wafers for 5 nm production; digital forensics tools that circumvent authentication or authorization controls on a computer (or communications device) and extract raw data; software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface; and sub-orbital craft. Due to COVID, the Wassenaar Arrangement did not convene its annual plenary in December 2020 and consequently no new controls were adopted. However, the United States will Chair the General Working Group of Wassenaar in 2021, and given the significant work completed by Commerce and other U.S. Government agencies over the past several years to identify emerging technologies for control, the United States will be well-positioned to push for new controls over the course of 2021 for adoption at the Plenary meeting in December 2021.

Commerce made one exception in 2020 to its policy of waiting to build international consensus before imposing U.S. controls on emerging technologies. On January 3, 2020 it imposed new export controls on artificial intelligence software that is specially designed to automate the analysis of geospatial imagery in response to emergent national security concerns related to the newly covered software. As a result, a license from Commerce is now required to export the geospatial imagery software to all countries, except Canada, or to release the software to foreign nationals employees working with the software in the United States. To impose the new control, Commerce 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. In early 2021, Commerce opted to extend this unilateral control for another year while it continues to work towards consensus with other countries to impose parallel controls.

2. Foundational Technology Controls

ECRA also mandates Commerce to identify and impose new export controls on foundational technologies, and Commerce released an Advance Notice of Proposed Rule-making ("ANPRM") on this topic in August 2020. However, in contrast to its more open-ended ANPRM on emerging technologies, in this request for comments, Commerce suggested that new, item-based controls on foundational technologies may not be warranted provided that their export is being controlled to certain destinations through other means. Specifically, Commerce noted that the expanded list of ECCNs it added to

the EAR's Military End User controls, which includes technologies that might be used by the governments of China, Russia, and Venezuela to build their respective defense industrial capabilities, could be deemed foundational technologies. Commerce also noted that it might draw on recent DOJ enforcement actions to help identify technologies that other countries have deemed critical enough to target for economic espionage. Overall, the approach taken in this ANPRM suggests that Commerce will be looking for other ways to impose controls on foundational technologies that would be less sweeping than the near globally-applicable, item-based licensing requirements it has imposed on the emerging technologies it has identified to date.

3. Removal of CIV License Exception

On June 29, 2020, as part of its efforts to curtail the export of sensitive technologies to countries that have policies of military-civil fusion, Commerce removed the license exception Civil End Users ("CIV") from Part 740 of the EAR, which 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 certain countries.

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 Commerce Control List ("CCL"). The countries included in this new restriction are from Country Group D:1, which 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 and 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 a country's military capacity contrary to U.S. national security interests.

4. Direct Product Rule Change

Although Commerce's initial expansion of its Entity List-based controls targeted Huawei, it may point the way toward other Entity List-based and new end-user and end use-based licensing controls in 2021. As noted above, to further constrain Huawei and its affiliates, Commerce created a new Entity List-specific rule that significantly expands the Direct Product Rule to include a wide range of software, technology, and their direct products, many of which used to develop and produce semiconductor and other items that Huawei uses in its products. We expect further experimentation with Entity List-based controls in 2021, including potentially, lowered the "De Minimis Rule" thresholds, which could greatly expand the range of foreign products incorporating controlled U.S. content that would require Commerce licensing when specific parties are involved.

5. Expanded Crime Control and Human Rights Licensing Policy

Commerce also focused efforts in 2020 on a review and update of controls imposed on U.S. origin items under its Crime Control policy. Most of the items controlled by the EAR for Crime Control reasons today are items that have been used by repressive regimes for decades, such as riot gear, truncheons, and implements of torture. In July 2020, Commerce issued a Notice of Inquiry signaling its intention to update the list of items to include advanced technology such as facial recognition software and other biometric surveillance systems, non-lethal visual disruption lasers, and long range acoustic devices. While, as of this writing, Commerce continues to work through the comments submitted in response to the Notice, on October 6, 2020 it imposed new controls on exports of water

cannon systems for riot and crowd control to implement a specific mandate from Congress to restrict the export of commercial munitions to the Hong Kong Police Force.

On the same day, Commerce amended the EAR to reflect a new licensing policy to deny the export of items listed on the Commerce Control List for crime control reasons to countries where there is either civil disorder or it assesses that there is a risk that items will be used in the violation or abuse of human rights. This amendment changed the Commerce Department's licensing policy in two ways. First Commerce licensing officers no longer require evidence that the government of an importing country *has* violated internationally recognized human rights. Instead, BIS will consider whether an export *could* enable non-state actors engage in or enable the violation or abuse of human rights.

Second, Commerce noted that it would extend its Crime Control review policy to proposed exports of other items that are not specifically listed on the CCL for Crime Control reasons. This second expansion is particularly noteworthy because it expressly allows Commerce licensing officers to consider human rights concerns when reviewing proposed exports of many other items used by repressive governments today to surveil and stifle dissent or engage in other kinds of human rights violations, such as more generally benign telecommunications, information security, and sensor equipment.

B. State Department

1. Directorate of Defense Trade Controls (DDTC)

There were far fewer legal or regulatory developments at DDTC than occurred at Commerce in 2020, and DDTC appeared to focus much more effort on several practice-related changes. Indeed, DDTC spent significant time to launch a single digital platform for the processing of registrations, license applications, and correspondence requests, among other submissions.

The most significant rule change came in January when DDTC issued its final rule to revise Categories I, II, and III of the United States Munitions List to remove from Department of State jurisdiction the controls on certain firearms, close assault weapons, and combat shotguns, other guns and armament, and ammunition. The Department of Commerce now regulates the export and reexport of the items transferred to the Commerce Control List going forward.

DDTC also implemented a long awaited change to the ITAR's export licensing treatment of encrypted communications on March 25, 2020. The rule change affords similar (but not thesame) treatment to encrypted communications as does the EAR and should make it easier for companies and other organizations to use Internet and international cloud networks to transmit and store encrypted ITAR technical data without triggering licensing requirements.

DDTC made greater use in 2020 of Frequently Asked Questions to provide guidance on a range of topics. Most significantly, the DDTC shared, in real time, its evolving policy on whether U.S. person nationals working outside of the United States and providing defense services need to maintain separate registrations and obtain ITAR authorizations in a series of FAQs published on January 8, February 21, and April 4. DDTC also issued FAQs providing guidance on its recently revamped "By or For" license exemption, 22 CFR § 126.4, which will make it significantly easier for U.S. Government contractors to export defense articles and defense services without ITAR authorization when these exports are being done at the direction of U.S. Government agencies and meet certain criteria. On October 20, DDTC used an FAQ to provide an explanation of a frequently invoked but not always clearly understood licensing rule referred to as the ITAR "see-through rule." Curiously, DDTC found it necessary to inform the exporting public in a May FAQ that Puerto Rico is in fact a U.S. territory, along with American Samoa, Guam, and the U.S. Virgin Islands, and did not require ITAR licensing.

2. Bureau of Democracy, Human Rights, and Labor

On September 30, the State Department Bureau of Democracy, Human Rights, and Labor issued due diligence guidance on transactions that might result in the sale of products and services with surveillance capabilities foreign government end-users (hereinafter "Guidance"). The non-binding Guidance tracks and applies human rights diligence international standards set out in the United Nations Guiding Principles and Organization for Economic Co-operation and Development (OECD) Guidelines for Multinational Enterprises to surveillance product and service transactions. State's surveillance guidance identifies "red flags" members of the regulated community should watch for prior to entering into a transaction with a government end-user, along with suggested safeguards—such as contractual provisions and confidential reporting mechanisms—to detect and halt rights abuses should they occur. Although the Guidance does not break new ground for many large manufacturers of these products that already incorporate human rights-related diligence in their evaluation of proposed sales of these products and services, sensitive jurisdictions, mid- and smaller-size firms might find it helpful. Especially for resource-constrained entities that may not know what resources might be available to inform their due diligence, the Guidance identifies specific U.S. and non-U.S. Government publications and tools. For those companies not yet conducting human rights diligence on transactions involving these products, the Guidance helps set the bar on the expectations that investors, non-government organizations, and other stakeholders have for their business conduct going forward.

IV. European Union

A. EU-China Relationship

In 2020, the EU charted a somewhat different course than Washington in its economic relations with China. It finalized a comprehensive agreement on investment focused on enabling an increase in outbound investment in China from the EU, and at the same time, EU and its member states enhanced their framework for reviewing foreign direct investment ("FDI") to address concerns regarding, *inter alia,* Chinese investments in certain sectors in the EU.

On December 30, 2020, the EU and China concluded negotiations for a Comprehensive Agreement on Investment ("CAI"). China has committed to a greater level of market access for EU investors, including opening certain markets for foreign investments from the EU for the first time. China has also made commitments to ensure fair treatment of investors from the EU, with the EU hoping for a level playing field in China (specifically vis-à-vis state owned enterprises), transparency of subsidies granted and rules against the forced transfer of technologies. China has also agreed to ambitious provisions on sustainable development, including certain commitments on forced labor and the ratification of certain conventions of the International Labor Organization. The EU has committed to a high level of market entry for Chinese investors and that all rules apply in a reciprocal manner. As next steps, China and the EU will be working towards finalizing the text of CAI, before then being submitted for approval by the EU Council and the European Parliament.

On October 11, 2020, Regulation (EU) 2019/452 of 19 March 2019 establishing a framework for screening of foreign direct investments into the EU (the "EU Screening Regulation") entered into force, marking the beginning of EU-wide coordination regarding FDIs among EU member states and the European Commission. While FDI screening and control remains a member state competency, the EU Screening Regulation increases transparency and awareness of FDI flows into the EU. (For details

on the EU Screening Regulation and the newly applicable EU-wide cooperation process, see our respective client alert of March 2019.)

A notable case of enforcing FDI control in particular with respect to China is the prohibition by the German government in December 2020 of the indirect acquisition of a German company with expertise in satellite/radar communications and 5G millimeter wave technology by a Chinese state-owned defense group. Germany has seen an increased number and complexity of foreign investments and takeover (attempts) over the past couple of years, especially by Chinese investors, which has resulted in a continuous tightening of FDI rules in Germany. For additional details on the developments in 2020 with regard to the German FDI rules, including an overview of the investment screening process in Germany, please refer to our client alerts in May 2020 and November 2020.

B. EU Sanctions Developments

Currently, the EU has over forty different sanctions regimes or "*restrictive measures*" in place, adopted under the EU's common foreign and security policy ("CFSP"). Some are mandated by the United Nations Security Council, whereas others are adopted autonomously by the EU. They can broadly be categorized in EU Economic and EU Financial Sanctions. Further, EU member states may implement additional sanctions. EU economic sanctions, broadly comparable to U.S. sectoral sanctions, are restrictive measures designed to restrict trade, usually within a particular economic sector, industry or market—e.g., the oil and gas sector or the defense industry ("EU Economic Sanctions").

EU financial sanctions are restrictive measures taken against specific individuals or entities that may originate from a sanctioned country, or may have committed a condemned activity ("EU Financial Sanctions"). These natural persons and organizations are identified and listed by the EU in the *EU Consolidated List of Persons, Groups and Entities Subject to EU Financial Sanctions* ("EU Consolidated List"), broadly comparable to U.S. Specially Designated Nationals ("SDN") listings.

It is noteworthy that, on a regular basis, third-party countries align with EU Sanctions, such as recently North Macedonia, Montenegro, Albania, Iceland and Norway with regards to the Belarus Sanctions.

For a full introduction into EU Sanctions, including the EU Blocking Statute, as well as, exemplary, the German export control regime, please take a look at a recent GDC co-authored publication, the International Comparative Legal Guide to Sanctions 2020.

While EU sanctions are enforced by EU member states, the EU Commission has announced that it plans to take steps to strengthen sanctions enforcement. On January 19, 2021, the EU Commission published a Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions titled "The European economic and financial system: fostering openness, strength and resilience" (the "Communication"). The Communication describes EU sanctions as "key instrument" playing a "critical role in upholding the EU's values and in projecting its influence internationally". To improve the design and effectiveness of EU sanctions, the EU Commission will from 2021 will conduct a review of practices that circumvent and undermine sanctions. It will further develop a database, the Sanctions Information Exchange Repository, to enable "prompt reporting and exchange of information between the Member States and the Commission on the implementation and enforcement of sanctions." In addition, the Commission is setting up an expert group of Member States' representative on sanctions and extra-territoriality and intends to improve coordination on certain cross-border sanctions-related matters between Member States. The Commission will also work with Member States to establish a single contact point for enforcement and implementation issues when there are cross-border implications.

To supervise the harmonized enforcement of EU sanctions, the EU Commission—among

other measures—plans to create a dedicated system to report sanctions' evasion anonymously, including a confidential whistleblowing system.

1. EU Human Rights Sanctions

On December 7, 2020, the Foreign Affairs Council of the Council of the European Union, adopted Decision (CFSP) 2020/1999 and Regulation (EU) 2020/1998, together establishing the EU's first global and comprehensive human rights sanctions regime ("EU Human Rights Sanctions") (as discussed in detail in our recent client alert). The EU Human Rights Sanctions will allow the EU to target individuals and entities responsible for, involved in or associated with serious human rights violations and abuses and provides for the possibility to impose travel bans, asset freeze measures and the prohibition of making funds or economic resources available to those designated.

EU Human Rights Sanctions mirror in parts the U.S. Magnitsky Act of 2012, and its 2016 expansion, the U.S. Global Magnitsky Human Rights Accountability Act as well as similar Canadian and United Kingdom sanction regimes. Notably, in contrast to the U.S. and Canadian human rights sanctions regimes, and similar to the United Kingdom human rights sanctions regime, the list of human rights violations does not include corruption.

While human rights violations have been subject to EU sanctions in the past, imposed on the basis of a sanctions framework linked to specific countries, conflicts or crises, the newly adopted EU Human Rights Sanctions are a significantly more flexible tool for the EU to respond to significant human rights violations. Although no specific individual or entity have yet been designated under the EU human rights sanctions, companies active in the EU should be mindful of this new sanctions regime and take it into consideration in their compliance efforts.

On December 17, 2020, the European Commission published the Commission Guidance Note of the Implementation of Certain Provisions of Council Regulation (EU) 2020/1998 ("Human Rights Guidance Note") regarding the implementation of certain provisions of the EU Human Rights Sanctions, advising on the scope and implementation in the form of 13 "most likely" questions that may arise and the respective answers.

2. EU Cyber Sanctions

On May 17, 2019, the EU established a sanctions framework for targeted restrictive measures to deter and respond to cyber-attacks that constitute an external threat to the EU or its Member States. The framework was expounded in two documents, Council Decision (CFSP) 2019/797 and Council Regulation 2019/796 (as discussed in detail in our previous client alert). In July 2020, the EU imposed its first ever sanctions listing related to cyber-attacks against Russian intelligence, North Korean and Chinese firms over alleged cyber-attacks. The EU targeted the department for special technologies of the Russian military intelligence service for two cyber-attacks in June 2017. Four individuals working for the Russian military intelligence service were sanctioned for their alleged participation in an attempted cyber-attack against the Organization for the Prohibition of Chemical Weapons in the Netherlands in April 2018. Further, North Korean company Chosun Expo was sanctioned due to suspicions of it having supported the Lazarus Group, which is deemed responsible for a series of major cyber-attacks and cybercrime activities worldwide. In addition, Chinese firm Haitai Technology Development and two Chinese individuals were sanctioned. The EU alleged cyber-attacks aimed at stealing sensitive business data from multinational companies. On October 22, 2020, the EU used the framework to impose further sanctions on two Russian officials and part of Russia's military intelligence agency (GRU) over a cyberattack against the German parliament in 2015.

The Council of the EU recently extended the EU Cyber Sanctions until May 18, 2021.

3. EU Chemical Weapons Sanctions

On October 12, 2020, the European Council decided to extend the sanctions concerning restrictive measures against the proliferation and use of chemical weapons by one year, until October 16, 2021. Such EU Chemical Weapons Sanctions were initially introduced in 2018 with the aim to counter the proliferation and use of chemical weapons which pose an international security threat. The restrictive measures consist of travel bans and asset freezes. Further, persons and entities in the EU are forbidden from making funds available to those listed. Currently, restrictive measures are imposed on nine persons and one entity. Five of the persons are linked to the Syrian regime and the sanctioned entity is understood to be the Syrian regime's main company for the development of chemical weapons. The remaining four of the nine persons are linked to the 2018 attack in Salisbury using the toxic nerve agent Novichok.

4. EU Iran Sanctions & Judicial Review

In January 2020, France, Germany and the UK (the "E3") issued a joint statement reaffirming their support to the JCPOA, repeating their commitment throughout the year, and roundly rejecting the United States' attempts to trigger a UN sanctions snapback. In September 2020, the E3 also warned the United States that its claim to have the authority to unilaterally trigger the so-called JCPOA snap-back mechanism that would have led to reimposing UN mandated nuclear-related sanctions on Iran would have no effect in law. On December 21, 2020, a Meeting of the E3/EU+2 (China, France, Germany, the Russian Federation, the United Kingdom, and the High Representative of the European Union for Foreign Affairs and Security Policy) and the Islamic Republic of Iran stressed that JCPOA remains a key element of the global nuclear non-proliferation architecture and a substantial achievement of multilateral diplomacy that contributes to regional and international security. The Ministers reiterated their deep regret towards the U.S. withdrawal and agreed to continue to dialogue to ensure the full implementation of the JCPOA. Finally, the Meeting also acknowledged the prospect of a return of the U.S. to the JCPOA, and expressed they were ready to positively address this move in a joint effort.

Regarding litigation, on October 6, 2020, the Court of Justice of the European Union ("CJEU") gave its long-awaited judgment in *Bank Refah Kargaran v. Council* (C-134/19 P), an appeal against the judgment of the General Court in T-552/15, raising the question of the EU Courts' jurisdiction in sanctions damages cases. By this judgment, the General Court dismissed the action by Bank Refah Kargaran seeking compensation for the damage it allegedly suffered as a result of the inclusion in various lists of restrictive measures in respect of the Islamic Republic of Iran.

In its judgment, the CJEU ruled that the General Court erred in law by declaring that it lacked jurisdiction to hear and determine the action for damages for the harm allegedly suffered by the appellant as a result of the Common Foreign and Security Policy ("CFSP") decisions adopted under Article 29 TEU. According to the CJEU, and in sync with Advocate General Hogan's Opinion delivered in that case in May 2020, the General Court's jurisdiction extends to actions for damages in matters relating to the CFSP. In fact, it is to be understood that jurisdiction is given for the award of damages arising out of both targeted sanctions decisions and regulations. However, the CJEU dismissed the appeal on account of the lack of an unlawful conduct capable of giving rise to non-contractual liability on the part of the EU and upheld the General Court's interpretation that the inadequacy of the statement of reasons for the legal acts imposing restrictive measures is not in itself sufficiently serious as to activate the EU's liability

5. EU Venezuela Sanctions

The EU's Venezuela Sanctions include an arms embargo as well as travel bans and asset freezes on listed individuals, targeting those involved in human rights violations, and those undermining democracy or the rule of law.

On January 9, 2020, the EU's High Representative, Josep Borrell, declared that the EU is "ready to start work towards applying additional targeted measures against individuals" involved in the recent use of force against Juan Guaidó, the president of Venezuela's National Assembly, and other lawmakers to impede their access to the National Assembly on January 5, 2020.

On November 12, 2020, the European Council extended sanctions on Venezuela until November 14, 2021, and replaced the list of designated individuals, which now includes 36 listed individuals in official positions who are deemed responsible for human rights violations and for undermining democracy and the rule of law in Venezuela.

Recently, the EU has issued a Declaration stating that it is prepared to impose additional targeted sanctions in response to the decision of the Venezuelan National Assembly to assume its mandate on January 5, 2021, on the basis of non-democratic elections.

6. EU Russia Sanctions & Judicial Review

Since March 2014, the EU has progressively imposed increasingly harsher economic and financial sanctions against Russia in response to the destabilization of Ukraine and annexation of Crimea. EU Russia Economic Sanctions continue to include an arms embargo, an export ban on dual-use goods for military use or military end-users in Russia, limited access to EU primary and secondary capital markets for major Russian state-owned financial institutions and major Russian energy companies, and limited Russian access to certain sensitive technologies and services that can be used for oil production and exploration. On December 17, 2020, the EU renewed such sanctions for six months. The EU Russia Economic Sanctions imposed in response to the annexation of Crimea and Sevastopol have been extended until June 23, 2021.

Russia has imposed counter-measures in response to EU Russia Economic and Financial Sanctions. In particular, Russia decided to ban agricultural imports from jurisdictions that participated in sanctions against Moscow. The measures included a ban on fruit, vegetables, meat, fish, milk and dairy products. On December 22, 2020, in response to new EU Russia Financial Sanctions imposed on Russians officials in connection with the poisoning of opposition leader Alexei Navalny, Russia imposed additional travel bans on representatives of EU countries and institutions.

As to related judicial review, on June 25, 2020, the CJEU dismissed appeals brought by ***VTB Bank*** (C-729/18 P) and ***Vnesheconombank*** (C-731/18 P) against the General Court's judgments confirming their inclusion in 2014 in the EU's sanctions list, which restricted the access of certain Russian financial institutions to the EU capital markets. The Court *inter alia* remarked that the measures were justified and proportionate because they were capable of imposing a financial burden on the Russian government, because the government might need to have to rescue the banks in the future.

On September 17, 2020, the CJEU rejected an appeal (C-732/18 P) brought by Rosneft (a Russian oil company) against the General Court's decision to uphold its 2014 EU listing (T?715/14). The CJEU confirmed the General Court's assessment that the measures were appropriate to the aims they sought to attain. More specifically, given the importance of the oil sector to the Russian economy, there was a rational connection between the restrictions on exports and access to capital markets and the objective of the sanctions, which was to put pressure on the government, and to increase the costs of Russia's actions in Ukraine.

Following the same line of reasoning as in a series of previous judgments by the EU Courts in 2018[1] and 2019,[2] the General Court decided in a number of new cases that certain individual listings on the EU's Ukraine sanctions list (which, *inter alia*, targets those said to be responsible for the "*misappropriation of State funds*") are unlawful because the EU has not properly verified whether the decisions of the Ukrainian authorities contained

sufficient information or that the procedures respected rights of defence. More specifically:

On December 16, 2020, the General Court annulled the 2019 designation of Mykola Azarov, the former Prime Minister of Ukraine (T-286/19). Mr. Azarov is no longer subject to EU sanctions after his delisting in March 2020. The Court ruled that the Council of the European Union had made an error of assessment by failing to establish that the Ukrainian judicial authorities had respected Mr Azarov's rights of the defence and right to judicial protection.

Earlier in 2020, on June 25, 2020, the General Court issued its judgment in Case T-295/19 *Klymenko v Council*, in which the Court held that it was not properly determined whether Mr Klymenko's rights of defence were respected in the ongoing criminal proceedings against him in Ukraine. In particular, the Council had not responded to or considered Mr Klymenko's arguments such as that the pre-conditions for trying him in his absence had not been fulfilled, he had been given a publicly appointed lawyer who did not provide him with a proper defence, the Ukrainian procedure did not permit him to appeal against the decision of the investigating judge, and he was not being tried within a reasonable time. Mr Klymenko was relisted in March 2020 and so remains on the EU sanctions list.

Furthermore, on September 23, 2020, with its Judgments in cases T-289/19, T-291/19 and T-292/19, the General Court annulled the 2019 designation of Sergej Arbuzov, the former Prime Minister of Ukraine, Victor Pshonka, former Prosecutor General and his son Artem Pshonka, respectively. All remain on the EU's sanctions list, because their designations were renewed in March 2020.

7. EU Belarus Sanctions

On August 9, 2020, Belarus conducted presidential elections and, based on what were considered credible reports from domestic observers, the election process was deemed inconsistent with international standards by the EU. In light of these events and acting with partners in the United States and Canada, the EU foreign ministers agreed on the need to sanction those responsible for violence, repression and the falsification of election results. In addition, EU foreign ministers called on Belarusian authorities to stop the disproportionate violence against peaceful protesters and to release those detained.

Shortly afterwards, on August 19, 2020 the EU heads of state and government met to discuss the situation and, in declarations to the press, President Charles Michel affirmed that the EU does not recognize the election results presented by the Belarus authorities and that EU leaders condemned the violence against peaceful protesters. On this occasion, EU leaders agreed on imposing sanctions on the individuals responsible for violence, repression, and election fraud. However, Cyprus opposed the adoption of measures by insisting that the EU should first agree on the adoption of restrictive measures against Turkey. This episode highlighted that a single EU member state or small group of EU member states can complicate EU foreign policy goals and push for trade-offs on unrelated matters.

Yet, restrictive measures were effectively imposed on October 2, 2020 against 40 individuals identified as responsible for repression and intimidation against peaceful demonstrators, opposition members and journalists in the wake of the 2020 presidential election, as well as for misconduct of the electoral process. The restrictive measures included a travel ban and asset freezing.

On November 6, 2020, the set of restrictive measures was expanded, and the Council of the EU added 15 members of the Belarusian authorities, including Alexandr Lukashenko, as well as his son and National Security Adviser Viktor Lukashenko, to the list of individuals sanctioned.

Lastly, on December 17, 2020, the set of restrictive measures was further expanded in

order to adopt 36 additional designations, which targeted high-level officials responsible for the ongoing violent repression and intimidation of peaceful demonstrators, opposition members and journalists, among others. The listings also target economic actors, prominent businessmen and companies benefiting from and/or supporting the regime of Aleksandr Lukashenko. Therefore, after three rounds of sanctions on Belarus, there are currently a total of 88 individuals and 7 entities designated under the sanctions' regime in place for Belarus.

8. EU North Korea Sanctions

On July 30, 2020, the EU North Korea Economic Sanctions targeting North Korea's nuclear-related, ballistic-missile-related or other weapons of mass destruction-related programs or for sanctions evasion were confirmed, and will continue to apply for one year, until the next annual review.

9. EU Turkey Sanctions

On December 10, 2020, EU leaders agreed to prepare limited sanctions on Turkish individuals over an energy exploration dispute with Greece and Cyprus, postponing any harsher steps until March 2021 as countries sparred over how to handle Ankara.

Josep Borrell, the High Representative of the European Union for Foreign Affairs and Security Policy, is now expected to come forward with a broad overview report on the state of play concerning the EU-Turkey political, economic and trade relations and on instruments and options on how to proceed, including on the extension of the scope of the above-mentioned decision for consideration at the latest at the March 2021 European Council.

10. EU Syria Sanctions – Judicial Review

On December 16, 2020, the General Court dismissed the applications of two Syrian businessmen, George Haswani (T-521/19) and Maen Haikal (T-189/19), to annul their inclusion on the EU's Syria sanctions list. In both cases, the General Court held that the Council of the European Union had provided a sufficiently concrete, precise and consistent body of evidence capable of demonstrating that both Applicants are influential businessmen operating in Syria.

Similarly, on July 8, 2020, the General Court rejected an application by Khaled Zubedi to annul his inclusion on the EU's Syria sanctions (T-186/19) and on July 9, 2020 the CJEU rejected an appeal by George Haswani (C-241/19 P). In both cases the Courts concluded that the Council of the European Union could appropriately demonstrate that both men were leading businessmen operating in Syria and that neither had rebutted the presumption of association with the regime of President Assad. Also, on December 2, 2020, the General Court dismissed Nader Kalai's similar application of annulment (T-178/19).

In addition, maintaining its established position on the subject, the CJEU dismissed a series of appeals brought before it by 6 Syrian entities, Razan Othman (Rami Makhlouf's wife), and Eham Makhlouf (vice-president of one of the listed entities) challenging the General Court's decision to uphold their 2016-2018 listings (see cases C-350/19 P; C?349/19 P, C-348/19 P, C?261/19 P, C?260/19 P, C?159/19 P, C?158/19 P and C?157/19 P, published on October 1, 2020). The CJEU held that the General Court was right to uphold the appellants' listings because the EU's Syria sanctions include membership of the Makhlouf family as a criterion on which a designation can be based. Considering that the Appellants were all found to be wholly or by majority owned by Rami Makhlouf, their assets were liable to be frozen without the need to demonstrate that they actively supported or had derived some benefit from the regime.

11. EU Egypt Sanctions – Judicial Review

On December 3, 2020, the CJEU delivered its ruling on Joined Cases C?72/19 P and C?145/19 P, concluding that the sanctions on deceased former Egyptian leader Hosni Mubarak and several members of his family should be lifted because of due process errors. The CJEU found that the Council of the EU took as its basis for listing Mr. Mubarak and his family members the mere existence of judicial proceedings against them in Egypt for misappropriation of State funds, *i.e.,* the decision of an authority of a third State. As the Council of the EU took assurances from Egyptian authorities that these rights were being observed when it should have independently confirmed that the legal protections were in place before designating the individuals, the CJEU found that the Council of the EU failed to verify whether that decision had been adopted in accordance with the rights of the defense and the right to effective judicial protection of the individuals listed.

Nevertheless, the asset freeze on the Mubarak family members will remain in place as the judgment only overturns the Council of the EU's decisions to impose sanctions on the family in 2016, 2017 and 2018. The 2019 and 2020 renewals of the original legal framework are still undergoing litigation.

C. EU Member State Export Controls

1. Belgium

On June 26, 2020 the Belgian Federal Parliament adopted of a resolution urging the government to prepare a list of countermeasures against Israel in case it annexes the occupied Palestinian territories.

2. France

On June 3, 2020, the Court of Appeal of Paris (international commercial chamber) issued its Judgment in *SA T v Société N*. The Court of Appeal dismissed an appeal by a French contractor seeking the annulment of an arbitral tribunal's award on the grounds that it had breached French international public policy by failing to take into account UN, EU and US sanctions. The tribunal had ordered the contractor to pay €1 million to an Iranian company following a dispute over the conversion of a gas field into an underground storage facility. The Court of Appeal concluded that UN and EU sanctions regulations constitute "*mandatory overriding provisions*."

On July 24, 2020, the French Cour de Cassation lodged a request for a preliminary ruling to the CJEU, regarding the interpretation of UN and EU Iran sanctions, and more specifically on questions concerning creditors' ability to take enforcement action against assets frozen by EU sanctions regulations (registered under Case C-340/20).

The French Court referred the questions to the CJEU in order to decide appeals brought in case Bank Sepah v Overseas Financial Ltd and Oaktree Finance Ltd.

On December 9, 2020, the French government published an Ordinance n° 2020-1544 in the Official Journal, which expands controls on digital assets as part of efforts to combat money laundering and terrorist financing.

3. Germany

The German Federal Court of Justice (*Bundesgerichtshof*) ("*BGH*") decided on August 31, 2020, that the procurement of materials for a foreign intelligence service, while circumventing EU Sanctions, fulfills the elements of a crime under section 18 para. 7 No. 1 of the Foreign Trade and Payments Act (*Aussenwirtschaftsgesetz*) ("*AWG*"). Espionage or affiliation with an intelligence service are not necessary to act "*for the intelligence*

service of a foreign power."

In the case, a man sold machine tools to Russian companies for around €8 million in seven cases between 2016 and 2018. The man's actual contractual partner—a member of a Russian intelligence service—subsequently supplied the machines to a Russian state-owned arms company for military use. The arms company operates in the field of carrier technology and develops cruise missiles. The machine tools are considered dual-use technology, and the sale and export of such items to Russia is prohibited since 2014 under the EU Russia Sanctions, specifically Regulation (EU) 883/2014 as amended.

The BGH decided that it is sufficient if the delivery of the machines is a result of the perpetrator's involvement in the procurement structure of foreign intelligence services. An organizational integration of the perpetrator into the foreign intelligence service is not required to justify the higher penalty of section 18 para. 7 No. 1 AWG (imprisonment of not less than one year) compared to the regular sentencing range of section 18 para. 1 AWG (imprisonment from three months up to five years) imposed for embargo violations under the AWG.

4. Latvia / Lithuania / Estonia

On August 31, 2020, Latvia, as well as Lithuania and Estonia, imposed travel bans on 30 officials including the President of Belarus Alexander Lukashenko, on the basis of their contribution to violations of international electoral standards and human rights, as well as repression against civil society and opposition to democratic processes. Following this designation, on September 25, 2020, the aforementioned EU Member States added 98 Belarusian officials to this list.

In November 2020, the aforementioned EU Member States proceeded to further designations. More specifically, Estonia and Lithuania imposed travel bans on an additional 28 Belarusian officials, and Latvia imposed a travel ban on 26 officials, all of whom are said to have played a central role in falsifying election results and using violence against peaceful protesters in Belarus. Overall, Latvia has now listed a total of 159 officials, who are banned from entering its territory indefinitely. Estonia and Lithuania have both listed 156 officials in total.

In February 2020, the Administrative Regional Court in Riga, Latvia rejected a request to suspend a ban issued by Latvia's National Electronic Mass Media Council on the broadcasting of 9 Russian television channels due to the designation of their co-owner, Yuriy Kovalchuck, who is listed pursuant to Council Regulation (EU) 269/2014 (undermining or threatening the territorial integrity, sovereignty and independence of Ukraine).

5. Luxembourg

On December 27, 2020, a law allowing Luxembourg to implement certain sanctions in financial matters adopted by the UN and the EU entered into force. The restrictive measures in financial matters envisaged by the law include asset freeze measures, prohibitions/restrictions of financial activities and financial services to designated people, entities or groups.

The measures can be imposed on Luxembourg nationals (residing or operating in or outside Luxembourg), legal persons having their registered office, a permanent establishment or their center of main interests in Luxembourg and which operate in, from or outside the territory, as well as all other natural and legal persons operating in Luxembourg.

Under this legislation, domestic supervisory and regulatory bodies are responsible for supervising the implementation of the law. This includes (i) the power to access any

documentation; (ii) request information from any person; (iii) request disclosure of communications from regulated persons; (iv) carry out on-site inspections; and (v) refer information to the State prosecutor for criminal investigation.

Failure to comply with the newly adopted restrictive measures shall be punishable by criminal penalties, such as imprisonment and/or a fine up to €5 million. Where the offence has resulted in substantial financial gain, the fine may be increased to four times the amount of the offence.

6. The Netherlands

On April 21, 2020, the Dutch Senate adopted an Act implemented amendments to the Fourth Anti-Money Laundering Directive (Directive EU 2015/849). This Act—which entered into force on May 18, 2020—provides that professional and commercial cryptocurrency exchange and wallet providers seeking to provide services in the Netherlands must register themselves at the Dutch Central Bank. For successful registration, adequate internal measures and controls to ensure compliance with EU and national (Dutch) sanctions must be demonstrated. Failure to show adequate sanctions compliance systems could lead to registration being denied, in which case such crypto companies would need to refrain from providing services. Further, the adoption in December 2019 by the Dutch Ministry of Foreign Affairs of guidelines for companies compiling an internal compliance programme (ICP) for "*strategic goods, torture goods, technology and sanctions*" is noteworthy. These guidelines resemble that of the EU's guidance aside from the inclusion of shipment control (rather than physical and information security) in its seven core elements.

7. Slovenia

On November 30, 2020, the Slovenian government issued a statement proscribing Hezbollah as a terrorist organisation, becoming the sixth EU member, after the Netherlands, Germany, Lithuania, Estonia, and Latvia to recognize the Iranian-sponsored Hezbollah as a terrorist organization.

8. Spain

On June 12, 2020, the Spanish Ministry of Economic Affairs and Digital Transformation published a Draft Law, amending Law 10/2010 of April 28 on the prevention of money laundering and terrorist financing, to transpose into Spanish domestic law the EU's Fifth Money Laundering Directive. The legislation also sets out the legal framework for enforcing compliance with EU and UN sanctions. More specifically, when it comes to the enforcement of sanctions, the Draft Law increases the limitation periods for sanctions: in the case of very serious offenses from three to four years, and in the case of serious offenses, from two to three years. In addition, fines will always be accompanied by other sanctions such as public or private reprimands/warnings, temporary suspensions or removals from office, while with the current Law 10/2010 this only occurs in case of sanctions for grave infractions.

C. EU Counter-Sanctions

The EU and its member states are also deeply concerned about the extraterritorial effects of both U.S. and Chinese sanctions and the recent approval of U.S. sanctions in relation to the Nord Stream 2 pipeline have further focused attention on this issue. With respect to Nord Stream 2, Josep Borrell affirmed that the EU does not recognize the extraterritorial application of U.S. sanctions and that it considers such conduct to be contrary to international law.

As discussed above, Germany has taken concrete steps to fend off the threat of U.S.

sanctions targeting the Nord Stream 2 pipeline. The German state of Mecklenburg-Vorpommern approved the establishment of the Mecklenburg-Vorpommern Climate and Environmental Protection Foundation (the "Foundation") to, *inter alia*, ensure the completion of the Pipeline, which is already more than 94% completed. While the declared aim of the Foundation is to counter climate change and to protect the environment (e.g., to avoid a pipeline run on the bottom of the ocean), the Foundation is also outspokenly designed to provide protection against U.S. sanctions by acquiring, holding and releasing necessary hardware to complete the Pipeline.

If successful, the move to shield companies or projects with state-owned/state-supported foundations might be copied by other governments in the EU, replacing or at least complimenting reliance on the EU Blocking Statute, which, at least in its current form, has been perceived as being insufficient to achieve its stated goal.

The EU has also been taking steps to provide itself with a toolkit that would allow to adopted block or counter non-EU sanctions with which it disagrees. A recent study requested by the European Parliament foreshadows possible upcoming counter sanctions and blocking measures aimed at defending the sovereignty of the European Union. The study suggests, for example, that EU businesses should be encouraged and assisted in bringing claims in international investor-state arbitration and in U.S. courts against sanctions imposed by the U.S. or other States and the blocking of financial transactions by the SWIFT system, which is constituted under Belgian law, subjected to European legislation and has been used in connection with the EU implementation of UN sanctions in the past. It remains to be seen if the EU will take onboard any of the suggestions put forward by the study.

Finally, on January 19, 2021, the EU Commission published a Communication to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions titled "The European economic and financial system: fostering openness, strength and resilience" (the "Communication"). The Communication notes that the EU plans to enforce the policy goals of the EU Blocking Statute through the general investment screening processes, which is enforced by the EU member states. Accordingly, U.S. investments in EU companies could be subject to more intense investment scrutiny if such investments could result in the EU target having to comply with U.S. extra-territorial sanctions.

According to the Communication, the EU Commission also plans to strengthen cooperation on sanctions, in particular with the G-7 partners. Also, the EU Commission will put in place measures to strengthen the Blocking Statute as the EU's most powerful tool to respond to sanction regimes of third countries, including (i) clearer procedures and rules; (ii) strengthened measures to block the recognition and enforcement of foreign decisions and judgments; (iii) streamlines processing for authorization requests; and (iv) possible involvement in foreign proceedings to support EU companies and individuals.

V. United Kingdom Sanctions and Export Controls

A. Sanctions Developments

1. New U.K. Sanctions Regime

Following the end of the Brexit Transition period on December 31, 2020, EU sanctions regulations are no longer being enforced by the U.K. However, the EU sanctions regime has been substantially retained in law in the U.K. through the introduction of multiple new U.K. sanctions regulations under the Sanctions and Anti-Money Laundering Act 2018 ("SAMLA"). The full list of these sanctions regulations can be found here. Certain of the new regulations relate to specific geographic regions (essentially those also subject to EU sanctions regimes). There are also a number of sanctions and related regulations imposing thematic sanctions (again, largely reflecting existing EU regimes), such as those relating to chemical weapons, terrorism, cybersecurity, human rights and kleptocracy.

The U.K. is also now maintaining the U.K. sanctions list, which provides details of all persons designated or ships specified under regulations made under SAMLA, the relevant sanctions measures which apply, and for U.K. designations, reasons for the designation. The U.K. sanctions list is updated in light of decisions making, varying or revoking a designation or specification. The U.K.'s Office of Financial Sanctions Implementation ("OFSI") maintains a consolidated list of persons and organizations under financial sanctions, including those under SAMLA and other U.K. laws. It should be noted that not all persons designated under EU sanctions regimes have been designated under the new U.K. regulations.

The new U.K. regime differs in certain modest, albeit significant ways, from the EU regime as implemented in the U.K. that went before. Perhaps the most significant of these is the fact that the U.K. sanctions regulations provide a greater degree of clarity than has been present to date in EU instruments as to the circumstances in which a designated person may "own or control" a corporate entity. The relevant provisions typically provide that a person will own or control a company where (s)he holds, directly or indirectly, more than 50 percent of its shares or voting rights or a right to remove or appoint the majority of the board, or where it is reasonable in all the circumstances to expect that (s)he would be able to "achieve the result that affairs of" the company are conducted in accordance with his/her wishes, by whatever means.

The geographic scope of liability under U.K. sanctions regimes is clarified by section 21(1) of SAMLA, and generally extends only to conduct in the U.K. or by U.K. persons elsewhere. Certain U.K. sanctions regulations contain provisions allowing the effect of the sanctions regulation in question to be overridden in the interests of national security or prevention or detection of crime; a provision which has no analogue in the EU sanctions instruments. "No claims" clauses of the kind typically present in EU sanctions regulations (i.e., provisions prohibiting satisfaction of a claim occasioned by the imposition of a sanctions regime) are not a feature of U.K. sanctions regulations.

The provisions in the U.K. sanctions regulations relating to asset-freezes also differ in certain limited, but material respects. For example, the provisions creating offences for breaches of asset-freezes require a prosecuting authority must prove that the accused had knowledge or reasonable cause for suspicion that (s)he was dealing in frozen funds or economic resources.

The framework for U.K. sanctions designations, administrative ministerial and periodic review of designations, and judicial challenges to designation decisions under Chapters 2 and 4 of SAMLA is now in effect.

2. New U.K. Human Rights Sanctions Regime

On July 9, 2020, the U.K. Government introduced into law in the U.K. the Global Human Rights Sanctions Regulations 2020 and began designating individuals under those regulations in connection with their alleged involvement in gross human rights violations. A link to our client alert on these Magnitsky-style sanctions can be found here.

3. The "U.K. Blocking Statute"

Following the end of the Brexit transition period, the EU Blocking Statute (Council Regulation No 2271/96) and related Commission Implementing Regulation 2018/1101) will no longer be directly applicable in the U.K., but will form part of the retained EU law applying in the U.K. through the Protecting against the Effects of the Extraterritorial Application of Third Country Legislation (Amendment) (EU Exit) Regulations 2020, which amends the Extraterritorial US Legislation (Sanctions against Cuba, Iran and Libya) (Protection of Trading Interests) Order 1996, the law which implemented the EU Blocking Statute. The explanatory memorandum to the 2020 Regulations can be found here, and related (albeit likely non-binding) summary guidance here.

It therefore remains an offence in the U.K. to comply with a prohibition or requirement imposed by the proscribed U.S. laws relating to Iran and Cuba, or by a decision or judgment based on or resulting from the legislation imposing the proscribed sanctions, and such decisions and judgments may not be executed in the U.K. The offence can be committed by anyone resident in the U.K., a legal person incorporated in the U.K., any legal person providing maritime transport services which is a U.K. national or (where for U.K.-registered vessels) controlled by a U.K. national, or by any other natural person physically present within the U.K. acting in a professional capacity.

4. U.K. Sanctions Enforcement in 2020

On February 18, 2020, OFSI published the fact that two fines totaling £20.47 million had been issued to ***Standard Chartered*** for violations of the Ukraine (European Union Financial Sanctions) (No. 3) Regulations 2014, which implemented EU Council Regulation 833/2014 imposing sanctions in view of Russia's actions in Ukraine. Article 5(3) of the EU Regulation prohibits any EU person from making loans or credit or being part of an arrangement to make loans or credit, available to sanctioned entities, where those loans or credit have a maturity of over 30 days. This enforcement action, which was in connection with loans made by Standard Chartered to Turkey's Denizbank, which was at the time owned almost to 100% Russia's Sberbank (then subject to restrictive measures), was OFSI's highest fine to date. The Report of Penalty can be found here.

The decision followed a review by the Economic Secretary to the Treasury under section 147 of the Policing and Crime Act 2017, which permits a party on whom a monetary penalty is imposed by the Treasury (of which OFSI forms part) under section 146 of that Act to request a review by the relevant minister. The Economic Secretary upheld OFSI's decision to impose two monetary penalties, but substituted smaller fine amounts. The fines originally imposed by OFSI were of £11.9 million and £19.6 million. The Economic Secretary reduced these to £7.6 million and £12.7 million. These numbers included a 30 percent reduction in accordance with OFSI's Guidance on Monetary Penalties to reflect the fact that Standard Chartered made a voluntary disclosure in this case. OFSI determined that this case should be considered in the 'most serious' category for fining purposes, allowing a maximum reduction of 30 percent.

The fine reductions granted by the Economic Secretary were on the basis of further findings that the bank did not willfully breach the sanctions regime, had acted in good faith, had intended to comply with the relevant restrictions, had fully co-operated with OFSI and had taken remedial steps following the breach. While these factors had been considered in OFSI's assessment, the Economic Secretary felt they should have been given more weight in the penalty recommendation.

B. Export Controls Developments

Following the end of the Brexit transition period, the domestic regime for exporting controlled goods (primarily military and dual-use items, and goods subject to trade sanctions) remains substantially unchanged in the U.K., save that the U.K.'s relationship with the EU and the equivalent EU regime will change. The Export Control Joint Unit ("ECJU") remains the body responsible for control and licensing exports of such items.

Under the Northern Ireland Protocol to the EU-U.K. Trade and Cooperation Agreement of December 30, 2020, EU regulations governing on export of controlled goods continue to apply in Northern Ireland.

Controls on the export of military items from the U.K. are largely unchanged; such exports remain subject to licensing, although open individual export licenses ("OIELs") exist for the export of military items from Great Britain (i.e., the U.K. excluding Northern Ireland) to the EU.

The former EU regime for export control of dual use items established under EU Regulation No 428/2009 is largely retained in English law through The Trade etc. in Dual-Use Items and Firearms etc. (Amendment) (EU Exit) Regulations 2019, the Export Control (Amendment) (EU Exit) Regulations 2020 and the Export Control Act 2002, which remains in force.

U.K. persons will now need an export license issued by the U.K. for exports of dual-use items from Great Britain to the EU, however, such exports are covered by a new open general export licence ("OGEL") published by the ECJU, which reduces the burdens for Great Britain exporters in having to apply for individual licenses. For exports of such items from the EU to the U.K., a license issued by an EU member state will now be needed, although it has been proposed by the European Council that the U.K. be added as a permitted destination under GEA EU001 to avoid licensing burdens for such exports.

An OGEL or individual export license to export dual-use items to a non-EU country issued by the U.K. remains valid for export from Great Britain. Registrations made with the U.K. for the EU General Export Authorisations ("GEAs") will continue to be valid for exports from Great Britain, as they will automatically become registrations for the retained GEAs. However, an export license issued by an EU member state will no longer be valid for export from Great Britain. Moreover, licenses issued by the U.K. will no longer be valid for export from an EU member state.

* * *

Finally, our entire team wishes you and yours health and safety during what continue to be very challenging circumstances. We recognize that the coronavirus pandemic has affected our clients and friends in different ways over the course of the last year—some have thrived, some are starting to rebuild, and others can never regain what has been lost. Our hearts go out to those who have struggled the most. We aim to be of service in the best and worst of times, and we certainly all hope for better days ahead in 2021.

---

[1] Judgment of the Court of Justice of the European Union of December 19, 2018 in case C?530/17 P, *Mykola Yanovych Azarov v The Council of the European Union*, para. 26, EU:C:2018:1031.

[2] Judgment of the General Court of the European Union of July 11, 2019 in cases T?244/16 and T?285/17, *Viktor Fedorovych Yanukovych v The Council of the European Union*, EU:T:2019:502; Judgment of the General Court of the European Union of July 11, 2019 in case T?274/18, *Oleksandr Viktorovych Klymenko v The Council of the European Union*, EU:T:2019:509; Judgment of the General Court of the European Union of July 11, 2019 in case T?285/18, *Viktor Pavlovych Pshonka v The Council of the European Union*, EU:T:2019:512.

The following Gibson Dunn lawyers assisted in preparing this client update: Judith Alison Lee, Attila Borsos, Patrick Doris, Markus Nauheim, Adam M. Smith, Michael Walther, Wilhelm Reinhardt, Qi Yue, Stephanie Connor, Chris Timura, Matt Butler, Laura Cole, Francisca Couto, Vasiliki Dolka, Amanda George, Anna Helmer, Sebastian Lenze, Allison Lewis, Shannon C. McDermott, Jesse Melman, R.L. Pratt, Patrick Reischl, Tory Roberts,

Richard Roeder, Sonja Ruttmann, Anna Searcey, Samantha Sewall, Audi Syarief, Scott Toussaint, Xuechun Wen, Brian Williamson, Claire Yi, Stefanie Zirkel, and Shuo Josh Zhang.

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)
Ronald Kirk – Co-Chair, International Trade Practice, Dallas (+1 214-698-3295, rkirk@gibsondunn.com)
Jose W. Fernandez – New York (+1 212-351-2376, jfernandez@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Marcellus A. McRae – Los Angeles (+1 213-229-7675, mmcrae@gibsondunn.com)
Adam M. Smith – Washington, D.C. (+1 202-887-3547, asmith@gibsondunn.com)
Stephanie L. Connor – Washington, D.C. (+1 202-955-8586, sconnor@gibsondunn.com)
Christopher T. Timura – Washington, D.C. (+1 202-887-3690, ctimura@gibsondunn.com)
Courtney M. Brown – Washington, D.C. (+1 202-955-8685, cmbrown@gibsondunn.com)
Laura R. Cole – Washington, D.C. (+1 202-887-3787, lcole@gibsondunn.com)
Jesse Melman – New York (+1 212-351-2683, jmelman@gibsondunn.com)
R.L. Pratt – Washington, D.C. (+1 202-887-3785, rpratt@gibsondunn.com)
Samantha Sewall – Washington, D.C. (+1 202-887-3509, ssewall@gibsondunn.com)
Audi K. Syarief – Washington, D.C. (+1 202-955-8266, asyarief@gibsondunn.com)
Scott R. Toussaint – Washington, D.C. (+1 202-887-3588, stoussaint@gibsondunn.com)
Shuo (Josh) Zhang – Washington, D.C. (+1 202-955-8270, szhang@gibsondunn.com)

Asia:
Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Fang Xue – Beijing (+86 10 6502 8687, fxue@gibsondunn.com)
Qi Yue – Beijing – (+86 10 6502 8534, qyue@gibsondunn.com)

Europe:
Peter Alexiadis – Brussels (+32 2 554 72 00, palexiadis@gibsondunn.com)
Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Nicolas Autet – Paris (+33 1 56 43 13 00, nautet@gibsondunn.com)
Susy Bullock – London (+44 (0)20 7071 4283, sbullock@gibsondunn.com)
Patrick Doris – London (+44 (0)207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly – London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Penny Madden – London (+44 (0)20 7071 4226, pmadden@gibsondunn.com)
Steve Melrose – London (+44 (0)20 7071 4219, smelrose@gibsondunn.com)
Matt Aleksic – London (+44 (0)20 7071 4042, maleksic@gibsondunn.com)
Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Richard W. Roeder – Munich (+49 89 189 33-160, rroeder@gibsondunn.com)

Related Capabilities

International Trade