GIBSON DUNN

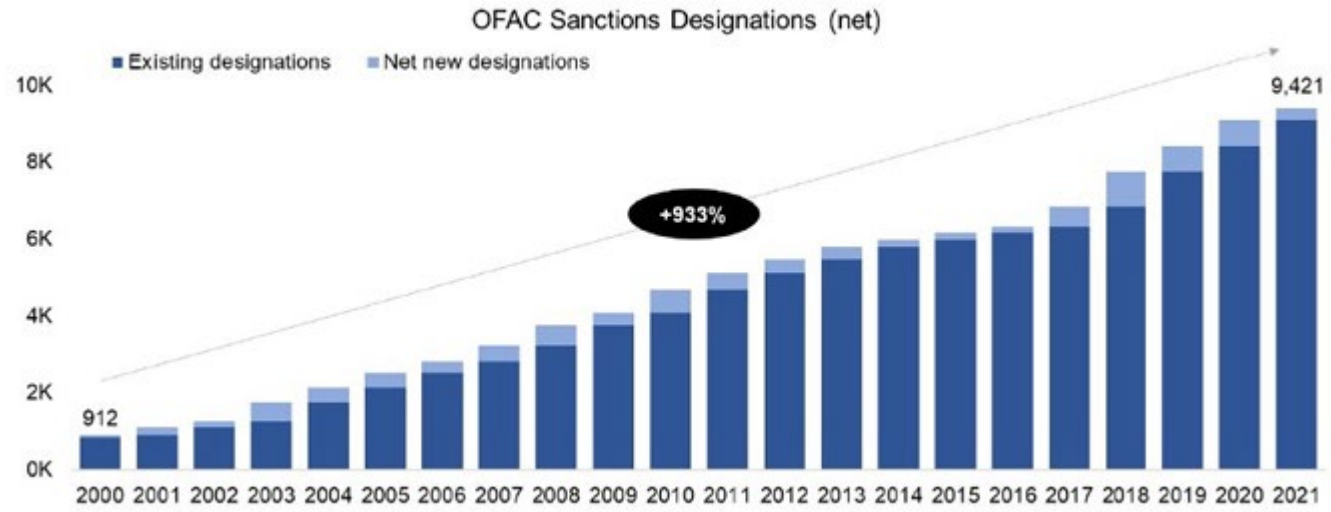
February 4, 2022

2021 YEAR-END SANCTIONS AND EXPORT CONTROLS UPDATE

To Our Clients and Friends:

The Biden administration made its mark on U.S. sanctions and export controls in 2021—reviewing, revising, maintaining, augmenting, and in some cases revoking various trade restrictive measures created during the Trump era. China remained at the forefront of the U.S. national security dialogue as the administration sought to solidify measures to protect U.S. communications networks and sensitive personal data and blunt the development of China's military capabilities after numerous earlier efforts by the Trump administration were blocked or limited by U.S. courts. China showed few signs of backing down in the face of U.S. pressure, instituting new restrictions that could potentially require multinational companies to choose between compliance with U.S. or Chinese law—creating a potential compliance minefield for global firms.

In October 2021, the U.S. Department of the Treasury published findings from its nine-month long review of the sanctions administered and enforced by the Office of Foreign Assets Control ("OFAC"), setting forth a policy framework to guide the imposition of new sanctions. The principles articulated in that review were apparent in major sanctions developments throughout the year—including new targeted sanctions on Myanmar, Belarus, and Ethiopia; the issuance of general licenses to facilitate the flow of humanitarian aid to Afghanistan after the Taliban takeover; termination of the sanctions with respect to the International Criminal Court; revocation of terrorist designations on the Revolutionary Armed Forces of Colombia ("FARC") and the Yemen-based Houthis; and the first designation of a virtual currency exchange for its role in facilitating ransomware payments. Negotiations over the future of the Joint Comprehensive Plan of Action ("JCPOA")—the 2015 Iran nuclear agreement abandoned by the Trump administration in 2018—continued, and the United States waived sanctions related to the Nord Stream 2 gas pipeline to appease European allies. In total, OFAC issued a total of 765 new designations and de-listed another 787 parties. By Treasury's own estimate, there were roughly 9,421 sanctioned parties by late 2021—a 933 percent increase since 2000.



Source: U.S. Dep't of Treasury, The Treasury 2021 Sanctions Review (Oct. 18, 2021)

OFAC sanctions developments tell only part of the story, as the United States continued to rely on export controls, foreign direct investment reviews, import restrictions, and restrictions with respect to the information and communications technology and services supply chain to accomplish foreign policy goals—often with a renewed emphasis on multilateral action. As in prior years, confronting the national security concerns associated with China remained a central focus of developments in U.S. export controls, especially those administered by the Department of Commerce's Bureau of Industry and Security ("BIS"). In addition to confronting national security challenges, BIS took substantial steps to update the Export Administration Regulations, including addressing concerns associated with emerging and foundational technologies. As of this writing, the United States and its European allies were hammering out the details of an aggressive package of sanctions and export controls targeting Russia should the Kremlin follow through on threats to further invade Ukraine—presenting a key test of the Atlantic alliance and the ability of multilateral trade controls to deter a threatened use of force.

Contents

I. U.S. Trade Restrictions on China

Despite the transition from the Trump to the Biden administration, U.S. trade policy toward China in 2021 was marked by a striking degree of continuity. As under the prior administration, the dozens of new China-related trade restrictions announced this year were generally calculated to advance a handful of longstanding U.S. policy interests for which there is broad bipartisan support within the United States, including protecting U.S. communications networks and sensitive personal data; slowing the advance of China's military capabilities; promoting human rights in Xinjiang and Hong Kong; and narrowing the bilateral trade deficit. As the Biden administration enters its second year in office and tensions between Washington and Beijing show few signs of abating, those core objectives of U.S. policy toward China appear unlikely to change, at least in the near term.

Meanwhile, as discussed more fully in Section VII, below, China this year deepened its already considerable efforts to resist U.S. pressure by adopting a host of new or expanded measures, including counter-sanctions, export controls, restrictions on cross-border data transfers, and a rigorous foreign investment review regime. In light of these new instruments in Beijing's policy arsenal, multinational enterprises seeking to do business in both of the world's largest economies now face the unenviable task of navigating between two competing, and often conflicting, sets of trade controls.

A. Protecting Communications Networks and Sensitive Personal Data

Spurred by concerns about Chinese espionage, the United States during 2021 sought to solidify trade restrictions designed to protect U.S. communications networks and sensitive personal data.

Notably, President Biden on June 9, 2021 issued Executive Order ("E.O.") 14034 to restrict the ability of "foreign adversaries," including the People's Republic of China, to access U.S. persons' sensitive data. That measure revokes three Executive Orders that targeted by name certain Chinese connected software applications, including ***TikTok*** and various mobile payment platforms. In place of those restrictions, E.O. 14034 articulates a more neutral set of criteria that U.S. Executive branch agencies are to use in evaluating threats to sensitive data of U.S. persons. The Order also sets forth a more rigorous process, including the preparation of two reports by the U.S. Secretary of Commerce, for recommending policy options to address the purported threat posed by such apps. From a policy perspective, these changes appear calculated to put the earlier, Trump-era restrictions on certain Chinese apps—which were effectively unenforceable, having been enjoined by multiple federal courts in September and October 2020—on firmer footing.

For a more detailed discussion of U.S. measures to secure information and communications technology and services against foreign interference, please see Section III, below.

B. Slowing the Advance of China's Military Capabilities

Another key feature of the Biden administration's trade policy in 2021 was its attempt to blunt the development of China's military capabilities, including by restricting exports of U.S.-origin items to certain Chinese end-users, prohibiting U.S. persons from investing in the securities of dozens of "Chinese military-industrial complex companies," and subjecting potential Chinese acquisitions of and investments in sensitive U.S. businesses to stringent foreign investment reviews.

Export controls this year remained a core element of U.S. efforts to slow Beijing's emergence as a strategic competitor as the Biden administration frequently used Entity List designations to target PRC-based firms. In its expanding size, scope, and profile, the Entity List has begun to rival OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List as a tool of first resort when U.S. policymakers seek to wield coercive authority, especially against major economies and significant economic actors. Among the more than 80 Chinese firms added to the Entity List during 2021 were substantial enterprises such as ***China National Offshore Oil Corporation Ltd.*** and the ***Xinjiang Production and Construction Corps ("XPCC")***.

Entities can be designated to the Entity List upon a determination by the End-User Review Committee ("ERC")—which is composed of representatives of the U.S. Departments of Commerce, State, Defense, Energy and, where appropriate, the Treasury—that the entities pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. Through Entity List designations, BIS prohibits the export of specified U.S.-origin items to designated entities without BIS licensing. BIS will typically announce either a policy of denial or *ad hoc* evaluation of license requests.

The practical impact of any Entity List designation varies in part on the scope of items BIS defines as subject to the new export licensing requirement, which could include all or only some items that are subject to the U.S. Export Administration Regulations ("EAR"). Those exporting to parties on the Entity List are also precluded from making use of any BIS license exceptions. However, because the Entity List prohibition applies only to exports of items that are "subject to the EAR," even U.S. persons are still free to provide many kinds of services and to otherwise continue dealing with those designated in transactions that occur wholly outside of the United States and without items subject to the EAR.

The ERC has over the past several years steadily expanded the bases upon which companies and other organizations may be designated to the Entity List to include activities like enabling human rights violations and producing surveillance technology. During 2021, BIS continued this trend by announcing six rounds of Entity List designations tied to activities in support of China's military. Among those designated in January, April, June, July, November, and December 2021 were more than 40 PRC entities for their alleged involvement in developing, for example, supercomputers, quantum computing technology, and biotechnology (including purported brain-control weaponry) for Chinese military applications.

As part of the growing use of export controls to slow the advance of China's military capabilities, 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, Venezuela, Burma, and Cambodia 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. 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.

The expanded Military End Use / User Rule has presented a host of compliance challenges for industry, prompting BIS in December 2020 to publish a new, non-exhaustive Military End User ("MEU") List to help exporters determine which organizations are considered military end users. The 71 Chinese companies identified to date appear to be principally involved in the aerospace, aviation, and materials processing industries. Although no new Chinese entities have been added to the MEU List since state-owned ***Beijing Skyrizon Aviation Industry Investment Co., Ltd.*** was named in the final days of the Trump administration, the Biden administration has continued to administer and enforce the MEU List (as well as the underlying Military End Use / User Rule). As such, that policy tool remains readily available and could be used by BIS in coming months to target additional entities with alleged links to China's security services.

In addition to expanding U.S. export controls targeting China, the Biden administration in June 2021 announced updated restrictions on the ability of U.S. persons to invest in publicly-traded securities of certain companies determined to operate in the defense and related materiel sector or the surveillance technology sector of China's economy.

In place of earlier Trump-era restrictions, an Executive Order promulgated on June 3, 2021—which OFAC is calling E.O. 13959, as amended—prohibits U.S. persons from engaging in "the purchase or sale of any publicly traded securities, or any publicly traded securities that are derivative of such securities or are designed to provide investment exposure to such securities" of certain companies named by the U.S. Secretary of the Treasury. In particular, persons may now be designated a Chinese Military-Industrial Complex Company ("CMIC") if they are determined by the Secretary of the Treasury: (1) to operate or have operated in the defense and related materiel sector or the surveillance technology sector of the economy of the People's Republic of China, or (2) to own or control, or to be owned or controlled by, such a company. The designation criteria in E.O. 13959, as amended, are therefore broader than under the Trump-era restrictions in that they target surveillance technology companies. Indeed, the White House has indicated that it intends to use E.O. 13959, as amended, to target Chinese companies that "undermine the security or democratic values of the United States and our allies"—including especially by targeting Chinese surveillance technology companies whose activities enable surveillance beyond China's borders, repression, and/or serious human rights abuses.

The investment restrictions set forth in E.O. 13959, as amended, take effect 60 days after a company becomes designated as a CMIC. U.S. persons have 365 days from a company's designation date to divest their interest in that CMIC. Those investment restrictions presently target 68 companies that appear by name on a new Non-SDN Chinese Military-Industrial Complex Companies List (the "NS-CMIC List") administered by OFAC. For the initial tranche of 59 companies that were added to the NS-CMIC List in June 2021, the investment restrictions came into effect on August 2, 2021, and U.S. persons have until June 3, 2022 to divest their interest in such firms.

From a policy perspective, the updated investment restrictions appear designed to provide greater clarity regarding precisely which PRC companies are being targeted. In that sense, E.O. 13959, as amended, seems to be a reaction to widespread market uncertainty concerning which entities were covered by the prior administration's restrictions, along with a series of successful court challenges by companies like the smartphone maker ***Xiaomi*** that were previously named on the basis of a surprisingly thin evidentiary

record. In our view, the updated restrictions appear calculated to put those earlier, Trump-era measures on firmer footing to withstand legal challenges—suggesting that the Biden administration is recalibrating investment restrictions targeting companies linked to China's military-industrial complex to survive for the long term.

Although the Entity List, the MEU List, and the NS-CMIC List are analytically distinct from one another, all three measures appear to be driven by similar concerns among U.S. officials regarding the use of U.S. resources—namely, technology and capital—to engage in activities contrary to U.S. national security interests, including facilitating the expansion of China's military capabilities. In addition to their shared policy underpinnings, the three lists are similar in that they are each tailored to restrict only certain narrow categories of transactions. Unlike a designation to OFAC's SDN List—which generally results in U.S. persons being prohibited from engaging in substantially all transactions involving a targeted entity—the three lists discussed above are each less sweeping in their effects. The Entity List and the MEU List both impose a licensing requirement on exports, reexports, and transfers of certain U.S.-origin goods, software, and technology to named companies, many of which are located in China. The NS-CMIC List restricts U.S. persons from having investment exposure to publicly-traded securities of certain named Chinese companies. In each case, absent some other prohibition, U.S. and non-U.S. persons are permitted to continue engaging in all other lawful dealings with the listed entities. In that sense, these three lists each offer a potentially 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.

Consistent with a whole-of-government approach to limiting China's access to sophisticated technologies with potential military applications, the United States during 2021 also leveraged the expanded authorities available to the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee") to target sensitive investments by Chinese acquirers. Notably, a lengthy CFIUS investigation led the South Korea-based chipmaker ***Magnachip Semiconductor Corporation*** in December 2021 to abandon its planned acquisition by a PRC-based private equity firm, suggesting that the Committee is likely to remain intensely focused on blunting efforts by Chinese buyers to acquire advanced technologies in general and semiconductors in particular.

Meanwhile, the U.S. Congress has in parallel sought to bolster the United States' ability to develop the technologies of the future. The U.S. Senate in June 2021 approved a sprawling bill authorizing approximately $250 billion in spending to better position the United States to compete technologically with China, including through investments in research and development and semiconductor manufacturing. The measure, called the United States Innovation and Competition Act of 2021 ("USICA"), passed the Senate by a wide bipartisan majority—suggesting that countering China's growing influence remains one of the few areas of agreement between congressional Republicans and Democrats. Debate over the USICA will soon shift to a conference committee between the Senate and the House of Representatives, where the measure is expected to undergo further changes during coming months. Although it is uncertain whether and in what form the bill will ultimately be approved by both chambers of Congress, in light of the bill's broad base of support—including from President Biden—some version of the USICA appears likely to be passed by Congress and signed into law later this year.

C. Promoting Human Rights in Xinjiang

During 2021, the United States continued to ramp up legislative and regulatory efforts to address and punish reported human rights abuses, including high-tech surveillance of Muslim minority groups and forced labor, in China's Xinjiang Uyghur Autonomous Region ("Xinjiang").

The Biden administration took a number of executive actions against Chinese individuals and entities implicated in the alleged Xinjiang repression campaign. In March and December 2021, OFAC—acting in concert with the European Union, the United Kingdom, and Canada— designated to the SDN List four current or former PRC government officials for their ties to mass detention programs and other abuses. In December 2021, OFAC followed up on those designations by adding to the NS-CMIC List a total of nine Chinese surveillance technology companies for their role in enabling surveillance beyond China's borders, repression, and/or serious human rights abuses. Specifically, OFAC on December 10, 2021 named China-based ***SenseTime Group Limited*** a CMIC for owning a company alleged to have developed facial recognition programs "that can determine a target's ethnicity, with a particular focus on identifying ethnic Uyghurs." The following week, OFAC on December 16, 2021 named a further eight Chinese technology companies to the NS-CMIC List for operating in the surveillance technology sector of China's economy and/or for owning or controlling such an entity. Those eight firms were similarly targeted for their alleged involvement in developing technologies that have been used to—and, some cases, were specifically designed to—track members of ethnic and religious minority groups in Xinjiang, including especially ethnic Uyghurs. In addition to enabling the biometric tracking and surveillance of minorities in China, a further risk factor for designation to the NS-CMIC List appears to be the export of such surveillance technologies to regimes with troubling human rights records, for which several of the entities identified by OFAC were cited.

In tandem with sanctions designations, the United States during 2021 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. Continuing a trend begun in October 2019, the ERC on two separate occasions this past year—in June and July 2021—added a total of 19 Chinese organizations to the Entity List for their involvement in human rights violations against Uyghurs, Kazakhs, and other members of Muslim minority groups in Xinjiang. Entities so designated included the silicon producer ***Hoshine Silicon Industry (Shanshan) Co., Ltd. ("Hoshine")*** and the Chinese state-owned paramilitary organization XPCC, each for participating in the practice of, accepting, or utilizing forced labor in Xinjiang.

Consistent with the Biden administration's whole-of-government approach to trade with China, the United States also used import restrictions—including multiple withhold release orders issued by U.S. Customs and Border Protection ("CBP") and enactment of the Uyghur Forced Labor Prevention Act—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,

or WRO, which requires the detention of such goods at any U.S. port. To overcome a WRO and have its goods released into the United States, the importer bears the burden of demonstrating by evidence satisfactory to the Commissioner of CBP that the goods were *not* made, in whole or in part, with a prohibited form of labor—which, as a practical matter, is a difficult showing to make.

After issuing a record number of withhold release orders during 2020, CBP in January 2021 continued its aggressive use of this policy instrument by imposing a region-wide WRO targeting all cotton products and tomato products produced in whole or in part in Xinjiang. In June 2021, CBP issued a company-specific WRO targeting silica-based products—which are commonly used in solar panels and electronics—made by the Xinjiang-based company Hoshine and its subsidiaries. Underscoring the degree to which U.S. trade controls targeting China overlap and intersect, Hoshine was concurrently added to the Commerce Department's Entity List, thereby constraining the company's ability to both source inputs from, and sell goods into, the U.S. market.

Concerns regarding the PRC's activities in Xinjiang appear to be shared by bipartisan majorities within the U.S. Congress. In December 2021, Congress passed and President Biden signed into law the Uyghur Forced Labor Prevention Act (the "Uyghur Act"), which in effect subjects *all* goods sourced from Xinjiang to a withhold release order. A key feature of that legislation is the creation of a rebuttable presumption—which takes effect on June 21, 2022—that all goods mined, produced, or manufactured even partially within Xinjiang are the product of forced labor and are therefore not entitled to entry at U.S. ports. Although the presumption can be overcome by "clear and convincing" evidence, the nature of which is to be articulated in formal guidance later this year, importers may face substantial practical hurdles to conducting due diligence into their supply chains as PRC entities have historically been unwilling to submit to audits of their labor practices. (Moreover, PRC entities may be prohibited by local law from cooperating with such requests in light of China's new counter-sanctions measures, discussed in Section VII, below.) In addition to imposing import restrictions, the new law also amends the Uyghur Human Rights Policy Act of 2020 to authorize the President to impose sanctions on persons determined to be responsible for serious human rights abuses in connection with forced labor. For a more detailed description of the Uyghur Act and its implications for companies doing business in or related to Xinjiang, please see our January 2022 client alert.

As a complement to the legislative and regulatory changes described above, the Biden administration published guidance to assist the business community in conducting human rights due diligence related to Xinjiang. On July 13, 2021, the U.S. Departments of State, Treasury, Commerce, Homeland Security, and Labor, together with the Office of the U.S. Trade Representative, issued an updated Xinjiang Supply Chain Business Advisory. That document spotlights practices by PRC authorities that the U.S. Government considers objectionable, including especially related to forced labor and mass surveillance. The Advisory identifies "red flags" that individuals or entities linked to Xinjiang may be using forced labor, including dealing in certain types of goods (such as cotton and polysilicon) or operating facilities located within or near known internment camps and prisons.

D. Promoting Human Rights in Hong Kong

As Beijing continued to tighten its grip on the Hong Kong Special Administrative Region, the territory remained an area of focus for U.S. sanctions policy under the Biden administration. Building on policy measures announced during the preceding year—including revocation of Hong Kong's special trading status under U.S. law, passage of the Hong Kong Autonomy Act, and the imposition of blocking sanctions against the territory's chief executive, Carrie Lam—2021 witnessed multiple rounds of Hong Kong-related sanctions designations. Among those added to the SDN List for their alleged involvement in eroding Hong Kong's autonomy were numerous current PRC government officials.

Additionally, the Biden administration on July 16, 2021 published a new Hong Kong Business Advisory that describes the potential financial, legal and reputational risks that can arise from operating in Hong Kong. The Advisory, which was timed to coincide with the one-year anniversary of the Hong Kong national security law, spotlights in particular the possibility of arrest under the national security law, warrantless electronic surveillance, and restrictions on the free flow of information. The Advisory also provides a helpful compilation of the U.S. legal authorities pursuant to which Hong Kong and mainland Chinese individuals and entities may be sanctioned and warns that U.S. businesses may suffer consequences for complying with those measures under China's new counter-sanctions law, which we discuss in more detail in Section VII.A, below.

E. Trade Imbalances and Tariffs

Also in 2021, the Biden administration continued to make broad use of its authority to impose tariffs on Chinese-made goods. This policy approach—which was launched during the Trump era—remains the subject of substantial and ongoing litigation at the U.S. Court of International Trade. Among the mechanisms that the new administration has employed to retain significant tariffs targeting Beijing is 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.

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 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.

As we predicted in our 2020 Year-End Sanctions and Export Controls Update, although the China 301 Tariffs were a hallmark of the Trump administration's trade policy, they have so far remained in place under President Biden and the new administration appears disinclined to relax those measures without first extracting concessions from Beijing.

II. U.S. Sanctions

A. Treasury Department Sanctions Review

In early 2021, the incoming Biden administration signaled its intent to evaluate the way the United States utilizes sanctions as a tool of foreign policy—often putting aside questions regarding the fate of a long list of Trump-era policies while the review was ongoing. The Treasury Department released the findings from its sanctions review in October 2021. In that document, Treasury articulates both the emerging challenges to the efficacy of sanctions as a national security tool, as well as a set of principles to guide U.S. sanctions policymaking in the future.

As part of a broader effort to ensure that sanctions—the use of which has sharply expanded during the past two decades—remain a durable and effective policy instrument, Treasury in its review emphasized that U.S. sanctions policies should be tied to clear, discrete objectives that are consistent with relevant Presidential guidance. To accomplish that goal, Treasury indicated that it would on a going-forward basis adopt the use of a structured policy framework—similar to the rigorous process that informs the use of force by the U.S. military—by asking whether a proposed sanctions action:

- supports a clear policy objective within a broader U.S. Government strategy;
- has been assessed to be the right tool for the circumstances;
- incorporates anticipated economic and political implications for the sanctions target(s), U.S. economy, allies, and third parties and has been calibrated to mitigate unintended impacts;
- includes a multilateral coordination and engagement strategy (where possible); and
- will be easily understood, enforceable, and, where possible, reversible.

These principles were broadly apparent in the sanctions policy decisions made by the U.S. administration throughout 2021 as OFAC often announced new sanctions actions in coordination with close U.S. allies and issued numerous humanitarian general licenses to minimize the collateral consequences of U.S. measures on vulnerable populations such as the people of Afghanistan.

B. Myanmar

As we wrote in February and April 2021, the Biden administration imposed new sanctions on Myanmar (also called "Burma") in response to the Myanmar military's coup against the country's elected civilian government on February 1, 2021. Since then, the military (called the "Tatmadaw") has maintained tight control over the country by, among other things, using lethal force on protesters, issuing a series of martial law orders, and imprisoning civilian leaders like State Counselor Aung San Suu Kyi. As the situation worsened, the Biden administration continued to enhance sanctions, notably opting for a targeted, list-based approach instead of jurisdiction-wide measures like those on Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine.

The turmoil in Myanmar marks an unfortunate echo of the past. Suu Kyi had been detained by the military in the 1990s and early 2000s and the international community, led by the United States, had previously responded with sanctions. Myanmar eventually moved toward democratization, with one key pivot point being the overwhelming victory of Suu Kyi's political party, the National League for

Democracy, in the country's November 2015 elections. As we noted back in May 2016, the U.S. Government responded by easing sanctions pressure on Myanmar, eventually dismantling the country-specific sanctions program administered by OFAC. While there was no longer a Myanmar sanctions program, in the ensuing years OFAC continued to sanction Myanmar-based actors under other programs targeting specific behaviors such as narcotics trafficking, weapons proliferation, and human rights abuses—with an emphasis on the military-linked perpetrators of violence against the Rohingya, a religious minority group, in 2016 and 2017.

In the wake of the February 2021 military coup, rather than revive the former Myanmar sanctions program, President Biden created a new one by issuing Executive Order 14014. Under this authority, OFAC may designate to the SDN List individuals and entities determined to be directly or indirectly causing, maintaining, or exacerbating the situation in Myanmar, and/or leading Myanmar's military or current government, or operating in the country's defense sector. Under E.O. 14014, OFAC may also designate the adult relatives of a designee, the entities owned or controlled by a designee, or those providing material support to a designee.

The breadth of the designation criteria in E.O. 14014 affords the administration considerable flexibility in selecting its targets. The Biden administration has taken full advantage. During the past year, OFAC has sanctioned, among others, leaders of the Tatmadaw and their relatives, military-run governmental entities and their leaders, and military-linked businesses operating across economic sectors.

The March 2021 designation of two military conglomerates—***Myanmar Economic Holdings Public Company Limited ("MEHL")*** and ***Myanmar Economic Corporation Limited ("MEC")***—is arguably the most consequential of the designations thus far. As we discussed in April 2021, by operation of OFAC's Fifty Percent Rule, the sanctioned status of MEHL and MEC automatically flows down to their dozens of majority-owned subsidiaries that play foundational roles throughout the country's economy, implicating the Myanmar-based operations of numerous foreign companies with touchpoints with the United States. Recognizing the potential collateral impact of targeting such key economic actors, OFAC issued a set of four general licenses authorizing the wind down of transactions involving MEHL or MEC for a set time period (which has since lapsed), and authorizing activities conducted by the U.S. Government and certain international organizations and non-profits.

It is also worth noting that OFAC in May 2021 designated the State Administrative Council (the "SAC"), the governmental body established by the Tatmadaw to govern Myanmar. The consequences of the SAC's designation have been challenging to discern for companies doing business in Myanmar that deal directly or indirectly with the government. In our view, some clarity can be gained by looking to OFAC's historical practices. When OFAC imposed sanctions on the Government of Venezuela, for example, it was explicit in the underlying authority, Executive Order 13884, that the entire Maduro regime was being targeted. The agency also promulgated numerous Venezuela-related general licenses to protect innocent third parties from what was a massively impactful measure. In contrast, the SAC designation, on its face, singled out one governmental entity, with no corresponding general licenses issued. The intended effect here appears to us to have been targeted, as opposed to sweeping, restrictions.

Over the past year or so, OFAC has designated 87 individuals and entities pursuant to E.O. 14014—not all at once but in recurring waves of designations, often prompted by particular atrocities committed by the Tatmadaw. President Biden has to date taken a calibrated and incremental approach to exerting economic pressure on Myanmar, but the tools used have been wide-ranging—extending beyond sanctions to include export controls, import controls, anti-money-laundering, and labor measures. Indeed, on January 26, 2022, the U.S. Departments of Treasury, State, Commerce, Labor, and Homeland Security, plus the Executive Office of the President, jointly published a Burma Business Advisory summarizing these measures and highlighting sectors, activities, and actors that the U.S. Government considers high risk. Absent dramatic developments on the ground, we would expect this gradual and whole-of-government approach to continue so long as the Tatmadaw remains in power in Myanmar. If the Biden administration decides to further increase pressure, the expected departure of major Western energy firms with a longtime presence in the country could soon open the way to sanctions on state-owned ***Myanmar Oil and Gas Enterprise***, or MOGE, which is a key source of revenue for the military regime in Yangon.

C. Russia

Russia featured prominently in President Biden's first year of foreign policy developments and challenges, as demonstrated by a range of sanctions actions aimed at the Kremlin. These actions—largely geared toward addressing Russia's meddling abroad, including the annexation of Crimea, foreign election interference, and the SolarWinds cyberattack—have been relatively measured to date, reflecting concerns about potential impacts on European allies. However, an open question as of this writing is whether the Russian military buildup along the Ukrainian border will escalate into a further incursion into Ukrainian territory, which could trigger the imposition of biting sanctions and export controls by the United States and its North Atlantic Treaty Organization ("NATO") allies.

1. Nord Stream 2

In May 2021, the Biden administration waived sanctions on ***Nord Stream 2 AG***, the Russian-controlled company developing the Nord Stream 2 gas pipeline between Russia and Germany, along with the company's chief executive. A State Department press release noted that the agency determined that, with respect to those two parties, "it is in the national interest of the United States to waive" sanctions authorized by the Protecting Europe's Energy Security Act of 2019. The waiver came at the behest of Germany, with which the Biden administration has sought to strengthen ties. However, the action drew sharp criticism within the United States, including from both sides of the aisle in the U.S. Congress. Opponents of the project contend that, once complete, the Nord Stream 2 pipeline could strengthen Russia's hand by positioning the Kremlin to withhold gas supplies from European consumers and deprive Ukraine of gas transit fees, a key source of government revenue. The waiver subsequently gave rise to a blockade by Senate Republicans of dozens of Biden administration national security-related nominations, as well as vigorous debate in the halls of Congress concerning the amount of discretion that should be afforded to the Executive branch in determining whether to impose further sanctions on Russia.

2. Navalny Sanctions

In two separate actions taken in March and August 2021, the United States imposed sanctions on Russia in response to the 2020 poisoning of the Russian dissident and activist Aleksey Navalny. The measures, which were implemented pursuant to the Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 and various other U.S. legal authorities, expanded on sanctions imposed three years earlier in connection with a similar chemical attack on Sergei Skripal in the United Kingdom.

The March 2021 action consisted of the designation to the SDN List of seven Russian government officials involved in the attack and Navalny's subsequent arrest and imprisonment. At the same time, the Department of Commerce added 14 entities to the Entity List based on their support to Russia's chemical and weapons of mass destruction industries, and the Department of State expanded existing sanctions against multiple individuals and entities in Russian's chemical weapons sector. In connection with this action, the U.S. Government is also now prohibited from providing foreign assistance or authorizing arms sales, arms sales financing, U.S. Government credit, and exports of national security-sensitive goods and technology to Russia. EAR license exceptions GOV, ENC, BAG, TMP, and AVS remain available, and the U.S. Government will consider licenses necessary for flight safety, certain deemed exports, exports to wholly owned subsidiaries of U.S. and foreign companies in Russia, and exports in support of government space cooperation on a case-by-case basis. Commercial end users, state-owned enterprises, and exports in support of commercial space launches are subject to a presumption of denial.

In August 2021, the State Department, acting pursuant to Executive Order 14024 (described below), imposed restrictions on two Russian Ministry of Defense scientific institutes and OFAC designated to the SDN List additional individuals associated with Russia's foreign intelligence agency, the Federal Security Service (commonly referred to by its Russian acronym, the FSB), for their role in the Navalny poisoning.

3. Russian Harmful Foreign Activities Sanctions

As described in more detail in an earlier client alert, the United States on April 15, 2021 announced a significant expansion of sanctions on Russia for a range of harmful foreign activities such as the annexation of Crimea and interference with U.S. elections. The sanctions included new restrictions on the ability of U.S. financial institutions to deal in Russian sovereign debt and the designation of more than 40 individuals and entities for supporting the Kremlin's malign activities abroad. The basis for these actions, Executive Order 14024, relied in large part on earlier Executive Orders and actions, but also expanded Treasury's authorities to, for example, designate the spouse and adult children of sanctioned individuals, which could enable the future targeting of members of the Russian oligarchy and their close relatives. Other provisions in these and related actions taken by the Treasury Department suggest the Biden administration stopped short of adopting more draconian measures such as blacklisting either Russia's sovereign wealth fund or the Russian government itself. Those policy options therefore remain available in the event of a further significant deterioration in relations between Washington and Moscow.

4. Possible Ukraine-Related Sanctions and Export Controls

Meanwhile, as tens of thousands of Russian troops continue in early 2022 to mass on the border with Ukraine, the United States and its NATO allies have threatened a barrage of sanctions and export controls should Russia mount a further invasion of its western neighbor. As diplomatic talks regarding the security of Eastern Europe unfold, the White House has suggested that the United States and its allies could respond to Russian military aggression in Ukraine by barring Russian access to the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") messaging system that underlies global financial transactions. Additional possible consequences such as sanctions on major Russian banks and stringent controls on exports to Russia of semiconductors and electronics—all of which the White House has suggested could be imposed within hours of a Russian incursion—could severely disrupt the global economy in the near term.

D. Belarus

In keeping with one of the key recommendations of the Treasury Department's sanctions review, discussed above, the United States, in close collaboration with the European Union, United Kingdom, and Canada, imposed coordinated sanctions against individuals and entities associated with the deterioration in democratic norms and human rights in Belarus. OFAC emphasized that this effort "reflects the United States' commitment to acting with its allies and partners to demonstrate a broad unity of purpose" because "sanctions are most effective when coordinated where possible with allies and partners who can magnify the economic and political impact."

On April 19, 2021, subject to a wind-down period that has since expired, OFAC revoked a longstanding general license that authorized U.S. persons to engage in certain transactions involving nine sanctioned Belarusian state-owned enterprises. As described by the U.S. Department of State, that authorization was withdrawn in light of the human rights record of Belarusian leader Aleksandr Lukashenka and his regime, including the ongoing detention of hundreds of political prisoners following the country's August 2020 presidential election.

Following the May 2021 forced diversion of a commercial airliner by the Lukashenka regime and the subsequent arrest of dissent journalist Raman Pratasevich—described by some observers as a state-sponsored hijacking—OFAC on June 21, 2021 designated an additional 16 individuals and five entities. Among those added to the SDN List were senior Belarusian government officials and government agencies, including the State Security Committee of the Republic of Belarus (the "Belarusian KGB") and its chairman. OFAC concurrently issued a general license authorizing U.S. persons to engage in certain transactions involving the Belarusian KGB in its administrative capacity such as complying with law enforcement actions and investigations.

To mark the one-year anniversary of Belarus' fraudulent presidential election, President Biden on August 9, 2021 signed Executive Order 14038 authorizing sanctions on Belarusian government agencies and officials, as well as individuals and entities determined to operate or have operated in certain identified sectors of the Belarusian economy. Targeted industries include the defense and related material, security, energy, potassium chloride (potash), tobacco products, construction, and transportation sectors, plus any other sector of the Belarusian economy that may subsequently be

determined by the U.S. Secretary of the Treasury. In parallel, OFAC designated a further 23 individuals and 21 entities, including numerous parties identified as "wallets" for Lukashenka and his regime.

In late 2021, relations between Minsk and the West continued to spiral downward as the Lukashenka regime encouraged waves of vulnerable migrants to transit Belarusian territory and cross into the European Union. Following this development, OFAC on December 2, 2021 added Belarus to the short list of countries (including Russia and Venezuela) that are subject to sectoral sanctions. In particular, OFAC issued Directive 1 Under Executive Order 14038 prohibiting U.S. persons from transacting in, providing financing for, or participating in other dealings in the primary and secondary markets for "new" debt with a maturity of greater than 90 days issued by the Ministry of Finance or the Development Bank of the Republic of Belarus. OFAC indicated in published guidance that these sectoral restrictions apply only to the two named entities (and not their subsidiaries), and that absent some other prohibition, U.S. persons may continue engaging in all other lawful dealings with those two entities. OFAC concurrently designated a further 20 individuals and 12 entities, and identified three aircraft as blocked property. These designations targeted parties that financially prop up the regime, and those implicated in the Lukashenka regime's smuggling of migrants into the European Union.

E. Iran

The advent of the Biden administration brought to the foreground the question of the future of the JCPOA. In 2021, events unfolded much as we anticipated in our 2020 Year-End Sanctions and Export Controls Update. Consistent with the interest that both President Biden and then-Iranian President Hassan Rouhani had signaled in returning to the JCPOA, negotiations resumed in April 2021 against a tense backdrop as Iran announced plans to begin enriching uranium to 60 percent purity. Tehran's unveiling of new centrifuges was soon followed by an explosion at the Natanz nuclear enrichment facility that has been widely attributed to Israeli sabotage.

Although talks initially appeared to progress, negotiations stalled following the June 2021 election of current Iranian President Ebrahim Raisi—a hardliner who was previously (and remains) designated to the SDN List. Raisi was initially targeted in 2019 for his role as head of the Iranian judiciary in overseeing human rights abuses and, in an earlier role as prosecutor general, participating in a "death commission" that ordered the extrajudicial killing of thousands of political prisoners. Since assuming the presidency, Raisi has expressed support for a return to the JCPOA, and indirect talks resumed at the end of November 2021.

Progress in the resumed negotiations remains limited, and Iran meanwhile continues to advance its nuclear program—a trend that U.S. and European officials have indicated is not sustainable. On January 20, 2022, Secretary of State Antony Blinken said that it is "really now a matter of weeks" to "determine whether or not we can return to mutual compliance with the agreement," a sentiment echoed by his French and German counterparts.

In the absence of a return to or renegotiation of the nuclear deal, the architecture of the Iran sanctions program has thus far not substantially changed since President Biden took office. However, OFAC continued to make use of its existing counter-terrorism authority to issue a significant set of designations

in September 2021 targeting Hizballah and Iran's Islamic Revolutionary Guard Corps-Qods Force. Both organizations had already been designated to the SDN List pursuant to OFAC's counter-terrorism authority. The new designations target individuals and companies providing financial support to them, including the operation of a network for smuggling and selling valuable commodities, including gold, electronics, and currency, and laundering the proceeds through the international financial system. This action suggests that, with or without progress in the JCPOA talks, OFAC is likely to continue using its existing authorities to target Iran's perceived malign activities.

F. Cuba

First established six decades ago following Cuba's Communist Revolution, U.S. sanctions on the regime in Havana have lately oscillated between easing under President Obama and tightening under President Trump. Despite early speculation that the Biden administration might seek a renewed thaw in relations with Havana, prospects for relaxed U.S. sanctions were dashed as the Cuban government in July 2021 cracked down on a wave of peaceful protects by Cuban citizens.

The Biden administration in July and August 2021 soon announced four rounds of sanctions against Cuban government entities and senior officials, including the country's defense minister, pursuant to OFAC's Global Magnitsky sanctions authority which targets perpetrators of serious human rights abuse and corruption. On August 11, 2021, OFAC and BIS jointly issued a fact sheet highlighting the U.S. Government's longstanding policy commitment to ensuring the free flow of information to the Cuban people. In the wake of these developments, U.S. sanctions on Cuba—including the country's designation as a State Sponsor of Terrorism by the outgoing Trump administration—have remained substantially unaltered over the past year and show few signs of changing in the near term as the United States enters a pivotal election year.

G. Ethiopia

On September 17, 2021, OFAC launched a new Ethiopia-related sanctions program in response to the ongoing humanitarian and human rights crisis in Ethiopia, particularly in the country's Tigray region. This program, which we discuss in depth in a recent client alert, authorizes OFAC to impose sanctions measures of varying degrees of severity without those sanctions necessarily flowing down to entities owned by sanctioned parties, suggesting that the United States is aiming to limit ripple effects on the Ethiopian economy.

Executive Order 14046 permits the Department of the Treasury to choose from a menu of blocking and non-blocking sanctions measures, allowing for a targeted application of restrictions. In keeping with recent Executive Orders of its kind, the criteria for designation under the E.O. are exceedingly broad. The Secretary of the Treasury can designate foreign persons for a wide range of activities related to the crisis in northern Ethiopia. These criteria range from obstructing access to humanitarian assistance and targeting civilians through acts of violence to being a political subdivision, agency, or instrumentality of the Ethiopian or Eritrean governments or of certain political parties. Upon designation of any such foreign person, the Secretary of Treasury may select from a menu of sanctions, including both blocking and non-blocking measures such as prohibiting U.S. persons from engaging in certain

transactions with sanctioned persons involving significant amounts of equity or debt instruments, loans, credit, or foreign exchange.

Notably, unlike nearly all other sanctions programs administered by OFAC, E.O. 14046 stipulates that OFAC's Fifty Percent Rule does not automatically apply to any entity "owned in whole or in part, directly or indirectly, by one or more sanctioned persons, unless the entity is itself a sanctioned person" and the sanctions outlined within the E.O. are specifically applied. OFAC has indicated in published guidance that E.O. 14046's restrictions do not automatically "flow down" to entities owned in whole or in part by sanctioned persons unless such persons appear by name on either OFAC's SDN List or the agency's Non-SDN Menu-Based Sanctions ("NS-MBS") List.

Concurrent with the announcement of its Ethiopia-related sanctions, OFAC issued three general licenses in recognition of the importance of ongoing humanitarian efforts to address the crisis in northern Ethiopia. These general licenses authorize a wide range of transactions and activities carried out by enumerated international organizations and non-governmental organizations to address this humanitarian and human rights crisis, as well as humanitarian trade in agricultural commodities, medicine, and medical devices.

Nearly two months after the program was created, OFAC announced its first (and so far only) round of Ethiopia-related designations on November 12, 2021, issuing blocking sanctions against four entities and two individuals. Among those targeted were the People's Front for Democracy and Justice, Eritrea's sole legal political party, and the Eritrean Defense Force ("EDF"), Eritrea's military. OFAC in making that announcement highlighted reports of EDF looting, sexual assault, killing of civilians, and blocking of humanitarian aid.

H. Other Sanctions Developments

1. Virtual Currency and Ransomware

OFAC this year intensified its focus on digital currencies and ransomware by issuing multiple rounds of industry guidance and announcing the first U.S. sanctions designation of a virtual currency exchange. As cybercrime and ransomware schemes proliferate, OFAC appears poised to continue pursuing investigations and enforcement actions in the virtual currency space.

The total dollar value of ransomware-related reports filed with the U.S. Department of the Treasury more than doubled in 2021 compared against the prior year, according to information published by Treasury's Financial Crimes Enforcement Network ("FinCEN"). As reported by FinCEN, financial institutions filed over 600 ransomware-related suspicious activity reports during the first half of 2021, and the average payment amount for ransomware-related transactions was over $100,000. Of course, the May 7, 2021, ransomware attack on the ***Colonial Pipeline***, the largest pipeline system for refined oil products in the United States, involved a much larger sum—nearly $5 million, paid via Bitcoin—and focused global attention on the connection between cybercrime and digital currencies.

At the end of 2020 and in early 2021, OFAC published two enforcement actions against virtual currency services providers, ***BitPay*** and ***BitGo***. BitPay, headquartered in Atlanta, provides a payment processing

solution for merchants to accept digital currency as payment for goods and services. While BitPay screened its direct customers, the merchants, against OFAC restricted party lists, the company failed to use information it received about the merchants' customers at the time of a transaction, including a buyer's name, address, email address, phone number, and Internet Protocol ("IP") address, to determine whether buyers were located in sanctioned jurisdictions. BitGo, headquartered in California, failed to use IP address information it obtained regarding its direct customers for security purposes to also determine whether its customers were located in comprehensively sanctioned jurisdictions.

Both enforcement actions demonstrate OFAC's expectation that best practices with respect to sanctions compliance, including IP address geo-blocking and sanctions list screening, apply to virtual currency services providers to the same extent as traditional financial institutions. Additional details on those two enforcement actions can be found in our February 2021 client alert.

On September 21, 2021, OFAC took more severe action against ***SUEX OTC*** ("SUEX"), a virtual currency exchange headquartered in Moscow, by adding SUEX to the SDN List, essentially barring SUEX from transactions that utilize the U.S. financial system and prohibiting U.S. persons from engaging in transactions involving the company. According to OFAC, SUEX facilitated transactions involving illicit proceeds from at least eight ransomware variants and over 40 percent of SUEX's known transaction history is associated with illicit actors. That action—which marked the first time that OFAC has designated a virtual currency exchange to the SDN List—was soon followed by the SDN designation of the ***Chatex*** virtual currency exchange in November 2021.

Underscoring the agency's heightened focus on this space, in addition to pursuing enforcement actions and blacklisting alleged bad actors, OFAC in September 2021 published an updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments. That document emphasizes that ransomware payments carry an elevated risk of dealing with prohibited parties. Expanding on earlier guidance, the Advisory also notes that, should an apparent sanctions violation occur in connection with a ransomware payment, OFAC will now take into account both the subject person's cybersecurity practices and whether the ransomware attack was timely self-reported to U.S. authorities in determining what enforcement response to impose. OFAC in October 2021 also published an industry-specific handbook, titled Sanctions Compliance Guidance for the Virtual Currency Industry, that provides a comprehensive overview of OFAC's sanctions programs, requirements, and resources for establishing a sanctions compliance program. Among other measures, OFAC suggests that virtual currency industry participants, consistent with a risk-based approach to sanctions compliance, consider implementing IP address geo-blocking, restricted party screening, and periodic "lookback" reviews after the agency adds new virtual currency addresses to the SDN List.

2. Reversal of International Criminal Court Sanctions

A major reversal of Trump-era sanctions policy occurred on April 5, 2021 when the Biden administration announced the revocation of Executive Order 13928, which had authorized sanctions against foreign persons determined to have engaged in any effort by the International Criminal Court ("ICC") to investigate, arrest, detain, or prosecute United States or any U.S. ally personnel without the consent of the United States or that ally. As previously mentioned in our 2020 Year-End Sanctions and Export

Controls Update, that earlier Executive Order came in retaliation for the ICC's 2020 announcement of a human rights investigation into potential war crimes committed by U.S. troops, the Taliban, and Afghan forces in Afghanistan. As part of the Biden administration's revocation, OFAC announced the elimination of the International Criminal Court-Related Sanctions Regulations and the removal from the SDN List of ICC Prosecutor Fatou Bensouda and Phakiso Mochochoko, the Head of the Jurisdiction, Complementarity, and Cooperation Division of the Office of the Prosecutor.

The reasoning for this reversal, according to the State Department, was that although the U.S. "maintain[s] our longstanding objection to the Court's efforts to assert jurisdiction over personnel of non-States Parties such as the United States and Israel," the new administration felt that those concerns "would be better addressed through engagement with all stakeholders in the ICC process rather than through the imposition of sanctions." Given that the ICC sanctions were enacted without coordination with or support from traditional U.S. allies, this action appears to have been part of the Biden administration's broader push to normalize and improve strained relationships between the United States and its foreign partners.

3. Taliban Sanctions and Impact on Afghanistan

In the wake of the Taliban's *de facto* takeover of Afghanistan in August 2021, two longstanding sets of U.S. sanctions substantially complicated efforts by outside aid organizations to deliver humanitarian relief to the Afghan people.

Although Afghanistan itself is not subject to comprehensive U.S. sanctions, the Taliban have since 2001 been designated pursuant to E.O. 13224, which is administered through the Global Terrorism Sanctions Regulations and targets named foreign individuals, groups, and entities "associated with" designated terrorists. U.S. persons are generally prohibited from engaging in transactions involving the targeted individuals and entities—referred to as Specially Designated Global Terrorists ("SDGTs")—and all property and interests in property of an SDGT that come within U.S. jurisdiction are frozen.

The Taliban's designation as an SDGT presents serious practical challenges now that, as of August 2021, the organization exercises *de facto* control over the Afghan state. By operation of OFAC's Fifty Percent Rule, the prohibitions on dealing with an SDGT (or other type of blocked person) extend to entities owned fifty percent or more in the aggregate by one or more SDGTs (or other type of blocked persons). That longstanding OFAC policy raises substantial questions as to whether the Taliban's status as an SDGT applies by operation of law to dealings involving the Government of Afghanistan or perhaps more broadly the entire jurisdiction of Afghanistan. OFAC between September and December 2021 issued six general licenses authorizing U.S. persons to engage in various transactions to facilitate the provision of humanitarian aid to the people of Afghanistan; however, there is increasing concern that such humanitarian-focused authorizations may not be sufficient to protect the country's fragile economy and the livelihoods of ordinary Afghans. While the accompanying guidance states that "[t]here are no OFAC-administered sanctions that generally prohibit the export or reexport of goods or services to Afghanistan, moving or sending money into and out of Afghanistan, or activities in Afghanistan," the agency remains firm that such transactions cannot "involve sanctioned individuals, entities, or property in which sanctioned individuals and entities have an interest," thereby leaving much of this ambiguity

unanswered. The paucity of guidance on this point is further complicated by the lack of precedent for the circumstance in Afghanistan in which a sanctioned terrorist entity has seized control of an entire state, thereby offering the private sector few other points of reference.

In addition to U.S. sanctions targeting SDGTs, Section 302 of the Antiterrorism and Effective Death Penalty Act of 1996 ("AEDPA") authorizes the U.S. Secretary of State to designate an organization as a Foreign Terrorist Organization ("FTO") based on its status as a non-U.S. organization engaged in "terrorist activity" that poses a threat to U.S. nationals or national security. Under AEDPA, the Secretary of State may designate FTOs after consultation with the Secretary of the Treasury and the Attorney General. AEDPA also authorizes the Secretary of the Treasury to require financial institutions to block funds in their possession or control in which a designated FTO maintains an interest. Section 303 of the Act makes it a crime for persons within the United States or under U.S. jurisdiction to knowingly provide material support to an FTO, which term encompasses nearly all forms of property, as well as the provision of services such as transportation. OFAC implements Section 302 of AEDPA through the Foreign Terrorist Organizations Sanctions Regulations. Presently, 75 organizations are designated FTOs. Although the Taliban is not itself an FTO as of this writing, various organizations closely affiliated with the Taliban, including the Haqqani Network, members of which now occupy key Afghan government posts, are subject to such restrictions.

Uncertainty regarding the applicability of these two sets of sanctions restrictions, together with de-risking by multinational financial institutions, appears to have exacerbated one of the worst humanitarian crises in modern history, with more than 20 million Afghans reportedly on the brink of famine. Afghan banks have closed and, while some financial services have resumed in key cities, currency is in short supply and the movement of funds even internally within Afghanistan is challenging. The Afghan government has scant official assets located domestically and, given the Taliban sanctions, the country has been shut off from its modest assets domiciled abroad.

Notably, OFAC has maintained a freeze on the approximately $9.4 billion of Afghanistan's foreign reserves located at the Federal Reserve Bank of New York, and to date has only issued general licenses that apply to the provision of medical and humanitarian aid to non-governmental instrumentalities. A significant degree of uncertainty remains for the private sector regarding to what extent it would be permitted to engage with anyone within Afghanistan, if at all, beyond the confines of applicable licenses.

4. Notable SDN De-Listings

Although OFAC continued to designate new sanctions targets at a steady clip, there were also a number of significant removals from the SDN List during 2021, highlighting that OFAC views sanctions as reversible and designed to change behavior. One of the most consequential recent de-listings took place in December 2021 when OFAC removed 274 individuals and entities associated with the Revolutionary Armed Forces of Colombia, or the FARC, from the SDN List. These entities and individuals had previously been designated under the Foreign Narcotics Kingpin Sanctions Regulations and the Global Terrorism Sanctions Regulations. However, according to the State Department, in acknowledgement of the fact that the FARC had formally dissolved and disarmed following the 2016 peace deal with the

Colombian government, it "no longer exists as a unified organization that engages in terrorism or terrorist activity or has the capability or intent to do so."

Another notable de-listing took place on February 16, 2021, when the State Department announced that it would be lifting the FTO and SDGT designations of the Yemen-based organization Ansarallah (commonly known as the Houthis) and its key leaders. The Houthis were designated just weeks earlier during the waning days of the Trump administration, triggering bipartisan concern about deepening the already significant practical challenges of delivering aid to the Yemeni people. This reversal, according to a State Department press release, came as "a recognition of the dire humanitarian situation in Yemen." However, recent attacks by the Houthis against the United Arab Emirates—a close U.S. partner and host to a major U.S. military installation—have led some observers to suggest that the organization's counter-terrorism designations should be reinstated.

In total, 787 persons and entities were removed from the SDN List during 2021, primarily as a result of the Foreign Narcotics Kingpin Sanctions Regulations removals and the Narcotics Trafficking Sanctions Regulation removals. These removals appear to be in accord with the underlying policy rationale of sanctions designations—namely, to alter the behavior of malign actors.

III. Information and Communications Technology and Services (ICTS)

During the past several years, the United States has increasingly used a novel and still evolving policy tool—controls on the information and communications technology and services ("ICTS") supply chain—to shield sensitive U.S. data and communications. Years of malicious cyber activities targeting the United States have exposed both the significance of the ICTS industry to the national security and foreign policy interests of the United States and the vulnerabilities deep in the ICTS supply chain. Because a supply chain is only as strong as its weakest link, the ICTS supply chain controls regime seeks to identify the vulnerabilities down the supply chain to ensure the integrity of the ICTS industry.

The ICTS supply chain controls regime is built upon a number of Executive Orders—each addressing separate yet interrelated topics such as software applications, supply chain security, and cybersecurity—as well as accompanying regulations, reports, and initiatives by several government agencies, including the Department of Commerce and the Department of Homeland Security ("DHS"). What results is an emerging regulatory regime that has the potential to bring about significant compliance challenges for global companies operating in the ICTS industry. Below we summarize the major developments from the past year.

A. Executive Order 13873: ICTS Supply Chain Framework

On May 15, 2019, acting under the authorities provided by the International Emergency Economic Powers Act—the statutory basis for most U.S. sanctions programs—then-President Trump issued Executive Order 13873 (the "ICTS E.O."), declaring a national emergency with respect to the ability of foreign adversaries to create and exploit vulnerabilities in the ICTS supply chain. The ICTS E.O. charged the Commerce Department with implementing a new regulatory framework to control risks in the ICTS supply chain. Although the Commerce Department published a Proposed Rule pursuant to the

ICTS E.O. in November 2019, there was not much movement in this new regulatory framework until the beginning of this year.

1. ICTS Interim Final Rule

Just one day before the Biden administration's start, on January 19, 2021, the Commerce Department published an Interim Final Rule establishing the processes and procedures that the Secretary of Commerce will use to evaluate ICTS transactions covered by the ICTS E.O. The Interim Final Rule provides the Department of Commerce with a broad, CFIUS-like authority to prohibit or unwind transactions or order mitigation measures. Specifically, it authorizes the Secretary of Commerce to prohibit ICTS transactions if the following three conditions are met:

First—The transactions must involve the acquisition, importation, transfer, installation, dealing in, or usage of certain ICTS. ICTS is broadly defined as any technology product or service used for the purpose of "information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display." Despite many commenters' requests to narrow the scope of the rules, the Commerce Department declined to provide categorical exemptions to specific industries or locations. Instead, the Commerce Department identified six main types of ICTS transactions that will fall under the scope of this rule, which include critical infrastructure, networks and satellites, data hosting or computing, surveillance or monitoring, communications software, and emerging technology.

Second—The ICTS must be designed, developed, manufactured, or supplied by companies owned by, controlled by, or subject to the jurisdiction or direction of a "foreign adversary." The Interim Final Rule identifies six specific "foreign adversaries": (1) China, including the Hong Kong Special Administrative Region; (2) Cuba; (3) Iran; (4) North Korea; (5) Russia; and (6) the Maduro regime of Venezuela. This list is subject to change, however—the Secretary of Commerce may revise the list to go into effect immediately without prior notice and comment. The "person owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary" may include:

- Any agent, representative, or employee of a foreign adversary;
- Any person who acts at the order, request, or under the direction or control of a foreign adversary, or of a person whose activities are directly or indirectly supervised, directed, controlled, financed, or subsidized in whole or in majority part by a foreign adversary;
- Any person who is a citizen or resident of a nation-state controlled by a foreign adversary;
- Any corporation, partnership, association, or other organization organized under the laws of a nation-state controlled by a foreign adversary; and
- Any corporation, partnership, association, or other organization that is owned or controlled by a foreign adversary, regardless of the location.

Third—The ICTS transaction must "pose an undue or unacceptable risk"—an area that affords the Secretary of Commerce much discretion. The Interim Final Rule outlined broad criteria which the Secretary of Commerce may consider in assessing potential risks posed by the ICTS transaction:

- The nature and characteristics of the ICTS at issue in the transaction, including technical capabilities, applications, and market share considerations;
- The nature and degree of the ownership, control, direction, or jurisdiction exercised by the foreign adversary over the design, development, manufacture, or supply at issue in the ICTS transaction;
- The statements and actions of the foreign adversary at issue in the ICTS transaction;
- The statements and actions of the persons involved in the design, development, manufacture, or supply at issue in the ICTS transaction;
- The statements and actions of the parties to the ICTS transaction;
- Whether the ICTS transaction poses a discrete or persistent threat;
- The nature of the vulnerability implicated by the ICTS transaction;
- Whether there is an ability to otherwise mitigate the risks posed by the ICTS transaction;
- The severity of the harm posed by the ICTS transaction on health, safety, and security, critical infrastructure, sensitive data, the economy, foreign policy, the natural environment, or National Essential Functions; and
- The likelihood that the ICTS transaction would in fact cause threatened harm.

Although the Interim Final Rule's detailed lists of definitions and factors were an improvement from the 2019 Proposed Rule, the Interim Final Rule still left much room for discretion in the application of each of the three tests. Between the publication in January 2021 and the planned effective date in March, a number of U.S. trade associations submitted letters to the Commerce Department noting their concerns regarding the Rule's sweeping scope and vague language and seeking to pause the Rule going into effect. Commentators also speculated as to the actions that the Biden administration might take to delay or reduce the impact of this midnight regulation from the prior administration. Despite the many doubts and unresolved questions, on March 22, 2021, the Interim Final Rule went into effect as planned.

2. Review Process

Under the Interim Final Rule, the Secretary of Commerce may initiate a review of an ICTS transaction at his or her own discretion or upon written request from an appropriate agency head. If an ICTS transaction meets the criteria above, the Secretary of Commerce will make an initial determination as to whether to prohibit the ICTS transaction or propose mitigation measures. Within 30 days of receiving a

notice of the Commerce determination, the parties may challenge the initial determination or propose remedial steps (such as corporate reorganization, disgorgement of control of the foreign adversary, or engagement of a compliance monitor). Upon review, the Commerce Department must issue a final determination stating whether the transaction is prohibited, not prohibited, or permitted subject to mitigation measures. The final determination is generally to be issued within 180 days of commencing the initial review.

This review process is similar to that of CFIUS—another tool that is designed to protect U.S. national security interests in transactions involving foreign entities. In fact, the Interim Final Rule exempts transactions that CFIUS is actively reviewing or has reviewed, possibly recognizing that the two set of reviews are intended to address similar risks. However, the Interim Final Rule warns "that CFIUS review related to a particular ICTS, by itself, does not present a safe harbor for future transactions involving the same ICTS that may present undue or unnecessary risks as determined by the [Commerce] Department." Under the current construction, the Commerce Department can get a second chance to review a transaction even if CFIUS finds that it does not have jurisdiction or that the national security risks involved in the transaction are not significant.

To date, no transaction review has officially begun. However, the Commerce Department has made clear its intent to actively implement the Interim Final Rule. On March 17, 2021, the Commerce Department announced that it served subpoenas on multiple unnamed Chinese companies that provide ICTS in the United States. This announcement was coupled with an unequivocal statement from the Secretary of Commerce Gina Raimondo that the "Biden-Harris Administration has been clear that the unrestricted use of untrusted ICTS poses a national security risk" and that "Beijing has engaged in conduct that blunts our technological edge and threatens our allies." On April 13, 2021, the Commerce Department followed up with another subpoena on an unnamed Chinese company. The fact that the only subpoenas served to date were to Chinese companies is telling—the scrutiny that CFIUS has shown toward transactions involving Chinese entities might hold true for the ICTS supply chain controls regime, as well.

3. Safe Harbor Licensing Process

The Interim Final Rule also suggested that the Commerce Department will set forth a procedure for parties to seek a license for a proposed or pending ICTS transaction. The license application review would be conducted on a fixed timeline, not to exceed 120 days from accepting an application, such that if the Department of Commerce does not issue a license decision within 120 days from accepting the application, it will be deemed granted. The Department of Commerce noted, however, that it would not issue a license decision on a transaction that would reveal sensitive information to foreign adversaries or others who may seek to undermine U.S. national security.

On March 29, 2021, the Commerce Department published a Proposed Rule seeking input on establishing licensing procedures for the ICTS supply chain controls regime, including a question concerning whether the licensing process should model that of a CFIUS notification or a voluntary disclosure to BIS. Unsurprisingly, the possibility of the Commerce Department going through license applications for countless ICTS transactions within 120 days garnered much concern regarding the practicality of

such an arrangement. While the Commerce Department was slated to publish procedures for a licensing process by May 19, 2021, this did not happen, and the Commerce Department has not communicated a new timeline or specific plan to do so.

B. Executive Order 14034: Connected Software Applications

On June 9, 2021, President Biden issued Executive Order 14034 (the "Applications E.O."), which revoked three Trump-era Executive Orders that targeted by name TikTok and various other applications developed by Chinese companies. Instead, the Applications E.O. directed the Secretary of Commerce to undertake further consideration of the risks posed by "connected software applications" under the ICTS Supply Chain regulations, including potential undue or unacceptable risk to the ICTS, critical infrastructure, or national security of the United States.

On November 26, 2021, the Commerce Department published a Proposed Rule seeking to amend the Interim Final Rule. The Proposed Rule suggested two main amendments. One was to revise the definition of ICTS to include "connected software applications." The definition of the term "connected software applications" would mirror the language in the Applications E.O.

Another was to provide for additional criteria that the Secretary of Commerce "may consider specifically when determining whether ICTS Transactions . . . that involve connected software applications present an undue or unacceptable risk." The new criteria articulated in the Proposed Rule are:

- Ownership, control, or management by persons that support a foreign adversary's military, intelligence, or proliferation activities;
- Use of the connected software application to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data;
- Ownership, control, or management of connected software applications by persons subject to coercion or cooption by a foreign adversary;
- Ownership, control, or management of connected software applications by persons involved in malicious cyber activities;
- A lack of thorough and reliable third-party auditing of connected software applications;
- The scope and sensitivity of the data collected;
- The number and sensitivity of the users of the connected software application; and
- The extent to which identified risks have been or can be addressed by independently verifiable measures.

The Commerce Department sought public comments on the effectiveness of the criteria, as well as the definition of various key terms, such as "ownership, control, or management"; "reliable third-party auditing"; and "independently verifiable measures." The public comments reiterated many of the concerns that industry raised for the Interim Final Rule, especially noting the broad and vague nature of certain criteria. Once the Commerce Department has reviewed the comments, we anticipate there may be further changes, revisions, and additions. Further information on what the Commerce Department views as "thorough and reliable third-party auditing" and "independently verifiable measures" is going to be particularly significant as companies develop compliance measures to minimize the risk of an ICTS review.

C. Executive Order 14017: Supply Chain Security

On February 24, 2021, President Biden signed Executive Order 14017 (the "Supply Chain E.O."), which seeks to prepare the United States to address vulnerabilities in U.S. supply chains against unexpected threats, including cyber-attacks and geopolitical and economic competition.

Section 3 of the Supply Chain E.O. initiated a 100-day process of reviewing and assessing the strengths and weaknesses of supply chains across key industries (i.e., semiconductor manufacturing and advanced packaging; large capacity batteries; critical minerals and materials; and pharmaceuticals and active pharmaceutical ingredients). On June 8, 2021, the White House issued a Report from the 100-day review. While the Report mostly focused on recommendations to develop domestic capacity and gain a competitive edge, it also recognized that "[t]he United States cannot address its supply chain vulnerabilities alone." For each key industry, the Report included the commitment to work with allies and partners—to promote production and investment and to strengthen supply chain transparency.

Section 4 of the Supply Chain E.O. also designated the Secretary of Commerce and the Secretary of Homeland Security to provide a report on supply chains for critical sectors and subsectors of the ICT industrial base within one year (expected by February 24, 2022). On September 20, 2021, BIS and DHS published a Request for Public Comments regarding priority areas for the U.S. ICT supply chains. The Request sought comments not only on the general resilience and capacity of American manufacturing supply chains, but also specific policy recommendations. Examples of policy recommendations (e.g., "sustainably reshoring supply chains and developing or strengthening domestic design, components, and supplies"; "cooperating with allies and partners to identify alternative supply chains"; and "building redundancy into domestic supply chains") provide some window into the agencies' preliminary inclinations.

On October 29, 2021, BIS hosted a public-private Virtual Forum regarding the Request for Public Comments, during which some of these policy options were discussed. The industry panelists, including the Telecommunications Industry Association and the Information Technology Industry Council, generally argued against restricting the ICT supply chain or requiring the disclosure of sensitive proprietary data in the name of security. They instead supported efforts to streamline supply chain security rules, leverage public-private dialogues, and cooperate with allies and partners. The public comments received will very likely shape how the ICTS supply chain controls regime will be enforced.

D. Executive Order 14028: Cybersecurity

On May 12, 2021, President Biden issued Executive Order 14028 (the "Cybersecurity E.O."), setting out an ambitious schedule of reviews and rulemakings with respect to cybersecurity of software provided to the U.S. Government. The Cybersecurity E.O. calls for the federal agencies to modernize their cybersecurity practices and for federal contractors to share more information on cyber incidents. Of relevance to the ICTS supply chain regime, Section 4 of the Cybersecurity E.O. notes that "[t]he development of commercial software often lacks transparency, sufficient focus on the ability of the software to resist attack, and adequate controls to prevent tampering by malicious actors" and thus charges the federal agencies to "rapidly improve the security and integrity of the software supply chain" of critical software sold to the government.

The requirements under the Cybersecurity E.O. apply only to federal agencies and contractors. However, in a statement announcing the Cybersecurity E.O., President Biden expressly "encourage[d] private sector companies to follow the Federal Government's lead" in adopting comparable measures because "federal action alone is not enough" to protect against cybersecurity risks. As a result, the standards established for government contractors may come to be seen as what is "reasonable" or "standard" cyber and supply chain security in other related data and technology protection domains. In fact, on September 30, 2021, the Commerce Department's National Institute of Standards and Technology ("NIST") published draft preliminary guidelines on improving software supply chain security, pursuant to the Cybersecurity E.O. (final publication expected by February 6, 2022). The guidelines are addressed to software producers including commercial-off-the-shelf product vendors, as well as software purchasers and consumers including non-federal agency organizations.

E. Transatlantic Dialogues

On September 29, 2021, the U.S.-EU Trade and Technology Council ("TTC") held its inaugural meeting. There, the TTC established ten working groups, one of which was tasked with "work[ing] towards ensuring security, diversity, interoperability and resilience across the ICT supply chain, including sensitive and critical areas such as 5G, undersea cables, data centers, and cloud infrastructure," as well as data security. The TTC expects the working group to "develop a common vision and roadmap for preparing the next generation of communication technologies." While the TTC is still in its beginning stages, there are growing expectations for the TTC's role given the broader willingness that governments on both sides of the Atlantic have shown to rebuild cooperation. Forthcoming discussions from the TTC working groups will likely have direct and indirect impact on the U.S. Government's stance on ICTS companies and transactions.

IV. U.S. Export Controls

A. Commerce Department

1. Military End Use / User Rule

The Department of Commerce tested a set of new tools and recalibrated old ones during the Trump administration with the aim of ensuring that dual-use U.S. products and technology are not used by

companies and other entities located in countries with military-civil fusion policies to help build out their military research and development and production capabilities. In a development reported in our May 2020 client alert, the Commerce Department amended the Military End Use / User Rule to more broadly restrict dual-use products and technology and to broaden the definition of who should be considered a military end user.

As discussed more fully under Section I.B, above, on December 23, 2020, BIS further amended the MEU Rule to add a new MEU List for purposes of identifying specific military end users in China, Russia, and Venezuela. While the MEU Rule previously restricted exports, reexports, or transfers of items subject to the EAR to military end users or for military end use in specific countries, this change marked the first time that BIS identified specific entities of concern. BIS issued the MEU List in partial response to a flood of advisory opinion and licensing requests submitted by exporters who were uncertain as to whether their counterparty was a military end user. Designation to the MEU List subjects an entity to the export controls applied to more traditional military end users and military end uses, including requiring export licenses for certain items subject to the EAR that otherwise would not require authorization to be exported to end users in MEU List countries.

While Commerce's issuance of the MEU List is welcome, frequent updates to the list in 2021 have meant that exporters, and others whose supply chain sourcing from MEU List countries requires the export of technology to suppliers, have needed to stay vigilant. Moreover, because the list is not exhaustive—exporters are still obligated to perform due diligence to determine whether they might be exporting to a military end user or for a military end use—compliance with the MEU Rule has become one of the most challenging aspects of export control counterparty diligence. Such challenges are compounded by China's growing body of laws and regulations, discussed in Section VII, below, that restrict the ability of PRC companies to comply with U.S. sanctions.

For reasons specified in greater detail below, Burma and Cambodia were added to the list of countries subject to MEU controls in March 2021 and December 2021, respectively. Although, to date, BIS has only identified specific military end users located in China and Russia.

2. Military-Intelligence End Use / User Rule

Efforts to curtail exports to military end users were further expanded effective March 16, 2021, when BIS issued similar regulations to cover certain military-intelligence end uses and end users ("MIEUs"). This action added to the EAR a new MIEU Rule, which places significant restrictions on exports for a "military-intelligence end use" or to a "military-intelligence end user" in Burma, Cuba, China, Iran, North Korea, Russia, Syria, and Venezuela. Cambodia was subsequently added to this list on December 9, 2021. Significantly, in addition to prohibiting exports to MIEUs without a license—applications for which are subject to a presumption of denial—this rule prohibits U.S. persons from providing "support" to specified MIEUs, even if such support does not involve items subject to the EAR. "Support" is broadly defined to include certain shipments and transfers involving any items destined for MIEUs, the facilitation of such shipments and transfers, and performing any contract, service, or employment that may benefit or assist MIEUs, including but not limited to, "[o]rdering, buying, removing, concealing, storing, using, selling, loaning, disposing, servicing, financing,

transporting, freight forwarding, or conducting negotiations in furtherance of." The breadth of the new MIEU Rule imposes significant responsibility on U.S. persons to conduct sufficient due diligence to get comfort that they are not directly or indirectly supporting MIEUs, even when non-U.S. goods are involved. In light of the substantial compliance challenges that the MIEU Rule presents for industry, some observers have speculated that BIS may during the year ahead look to create a non-exhaustive MIEU List—similar to the MEU List that was introduced in December 2020—to help exporters determine which organizations are considered military-intelligence end users.

3. Sudan Moved to Less Restrictive Country Group B

On January 19, 2021, BIS removed anti-terrorism ("AT") controls on Sudan in conjunction with the State Department's rescission of Sudan's designation as a State Sponsor of Terrorism. This action moved Sudan from Country Group E:1 to Country Group B, substantially reducing export restrictions applied to the country and raising the *de minimis* level of foreign-manufactured goods incorporating U.S.-origin content that can be exported, reexported, or transferred to Sudan from 10 percent to 25 percent. However, Sudan still remains subject to arms control limitations due to its continued placement in Country Group D:5, and exports to Sudan are not eligible for License Exceptions GBS and TSR.

4. Burma Added to More Restrictive Country Group D:1

In the wake of the February 2021 military coup in Burma, BIS on February 17, 2021 suspended license exceptions LVS, GBS, TSR, and APP for exports to Burma, which due to Burma's Country Group B placement, would otherwise have been available. Pressure on the Burmese government was increased on March 8, 2021, when BIS moved Burma from Country Group B to Country Group D:1, a more restricted control group based on national security concerns. This designation removes several license exceptions that were previously available to Burma and subjects the country to the more restrictive national security licensing policy. Additionally, as noted above, the MEU Rule and MIEU Rule were extended to include military end uses and end users within that country in a further effort to restrict Burma's access to U.S.-origin goods. The ERC concurrently designated to the Entity List four substantial Burmese entities, including the country's Ministries of Defense and Home Affairs, plus the military conglomerates MEC and MEHL. Additional Entity List designations of four Burmese entities associated with copper mining followed on July 6, 2021.

5. Cambodia Subjected to More Restrictive Licensing Policy

Reflecting growing concerns among U.S. policymakers regarding Cambodia's deepening ties with the Chinese military, as well as allegations of corruption and human rights abuses leveled against the Cambodian government, BIS on December 9, 2021 amended its license policy for Cambodia by adding a presumption of denial for national security ("NS") controlled items that could be diverted to a military end user or military end use. As part of that same action, BIS added Cambodia to Country Group D:5, thereby subjecting the country to a U.S. arms embargo.

6. BIS Eases Restrictions of Exports of Vaccines

On January 7, 2021, BIS amended the EAR to clarify the scope of export controls that apply to certain vaccines and medical products. This update was meant to more closely align the controls under the EAR with the release (i.e., exclusion) notes in the "Human and Animal Pathogens and Toxins for Export Control" common control list published by the Australia Group—a multilateral forum consisting of 42 participating countries and the European Union that maintain export controls on a list of chemicals, biological agents, and related equipment and technology that could be used in a chemical or biological weapons program. The January 2021 rule made a number of technical changes to Export Control Classification Number ("ECCN") 1C991 in an attempt to clarify the controls that apply to certain vaccines. Most notably, the rule amends the vaccine controls in paragraph (a) of ECCN 1C991 to more closely align with the Australia Group release notes to minimize controls on certain vaccines (though AT controls still apply), which is expected to help facilitate the development of new vaccines. Additionally, the changes clarify that the more stringent chemical/biological ("CB") controls which apply to medical products described under ECCN 1C991.c do not also apply to medical products described under ECCN 1C991.d. As a result of this rule change, some COVID vaccines containing genetic elements of items controlled by ECCN 1C353 are now controlled under ECCN 1C991, which permits their export to all countries except for those subject to AT controls (as of this writing, Iran, North Korea, and Syria).

7. Implementation of Wassenaar Arrangement Controls

As discussed in greater detail in our 2020 Year-End Sanctions and Export Controls Update, on January 3, 2020, BIS imposed new unilateral export controls on artificial intelligence software specially designed to automate the analysis of geospatial imagery through an interim final rule, designating such items under the rarely-used temporary ECCN 0Y521. Under 15 C.F.R. § 742.6(a)(8)(iii), such items remain so classified for only one year, but the classification can be extended for two additional one-year periods. BIS utilized these extensions in January 2021 and again in January 2022 with the hope that it can persuade fellow Wassenaar Arrangement ("WA") members to adopt their own controls on this technology once the WA Plenary, which has been postponed due to pandemic-related travel restrictions, is able to meet again. The next plenary session is scheduled to convene in Vienna in December 2022. Through its participation in the 42-member WA, the United States seeks to advance national and international security and foreign policy objectives through the promotion of multilateral controls over the use and transfer of conventional arms and dual-use goods and technologies.

As part of its membership in the WA, the United States commits to implement certain mutually agreed-upon export controls, including controls on cybersecurity items, which have been actively under discussion by WA members since 2013. On October 21, 2021, BIS solicited comments on an interim final rule that would establish new NS and AT controls on most cybersecurity items—implementing in part controls agreed upon by WA members in 2013 and further modified in 2017. As part of this interim final rule, BIS also solicited comments on a revised License Exception Authorized Cybersecurity Exports ("ACE"), which would authorize exports, reexports, and transfers of cybersecurity items to most destinations and for many end users and end uses, so long as such items were not subject to surreptitious listening ("SL") controls under Category 5 – Part 2 of the Commerce Control List ("CCL"). While the proposed rule was meant to go into effect on January 19, 2022, BIS subsequently delayed implementation of the rule until March 7, 2022. BIS cited potential modifications to the rule as the

reason for the delay and credited the public comments the agency received for prompting certain reconsiderations—underscoring the importance of public comments in agency deliberations.

On March 29, 2021, BIS also implemented revisions to the CCL to implement changes from the December 2019 WA Plenary meeting. These changes included revisions to 22 ECCNs and eliminated encryption reporting requirements under License Exception ENC in the following circumstances: (1) eliminates the email notification requirement for 'publicly available' encryption source code and beta test encryption software, except for 'publicly available' encryption source code and beta test encryption software implementing "non-standard cryptography"; (2) eliminates the self-classification reporting requirement for certain 'mass market' encryption products under 15 C.F.R. § 740.17(b)(1); and (3) allows self-classification reporting for ECCN 5A992.c or 5D992.c components of 'mass market' products (and their 'executable software'). While this rule does not change License Exception ENC requirements for any non-'mass market' encryption item or for any encryption items that implement "non-standard cryptography," it has eliminated filing requirements for many companies using standard cryptography and has lightened the burden on others.

8. Emerging and Foundational Technology Controls

The Commerce Department's Emerging Technology Technical Advisory Committee held partially closed meetings on March 19, May 21, and October 28, 2021. The announced topics included discussions of public comments, as well as presentations on cyber defense, foreign engagement risks in research enterprise, and work at the human-technology frontiers—signaling the broad approach that BIS is taking to fulfill its mandate under the Export Control Reform Act of 2018 to establish controls on emerging and foundational technologies. As part of this effort, on October 5, 2021, BIS published a final rule to implement a decision from the Advisory Committee's Virtual Implementation session held in May 2021 to add controls on nucleic acid assembler and synthesizer "software" that is capable of designing and building functional genetic elements from digital sequence data. This software was identified as an emerging technology by BIS and given new ECCN 2D352.

In 2021, BIS continued its efforts to engage the public as it continues to assess the appropriate level of controls that should be applied to emerging and foundational technologies. On October 26, 2021, BIS issued an advance notice of proposed rulemaking ("ANPRM") to solicit comments on the potential application of export controls to brain-computer interface ("BCI") technology, including, among other things, neural-controlled interfaces, mind-machine interfaces, direct neural interfaces, and brain-machine interfaces. Previously, on November 19, 2018, BIS issued a similar ANPRM to broadly address a longer list of potential emerging technologies, including BCI technology. In this new ANPRM, BIS requested responses to a series of questions tailored specifically to BCI technology, signaling that the agency may be especially focused on placing export controls on such technology in the near future.

9. Solicitation of Public Comments on Issues Related to Supply Chains

As noted above, on February 24, 2021, President Biden issued Executive Order 14017 to address concerns associated with U.S. supply chains. As part of this E.O., the Secretary of Commerce was directed to submit reports on (1) the semiconductor manufacturing and advanced packaging supply

chains and policy recommendations to address these risks and (2) the supply chains for critical sectors and subsectors of the information and communications technology industrial base.

In an effort to implement these measures, BIS solicited comments from the public on March 15, 2021 (concerning semiconductor manufacturing and advanced packaging supply chains); September 20, 2021 (concerning ICT supply chains); and September 24, 2021 (concerning technical questions associated with the semiconductor product supply chain). On January 25, 2022, the Department of Commerce released the results of its semiconductor supply chain request for information, which provided an overview of some of the underlying causes of supply shortages and committed the agency to "engage industry on node-specific problem-solving in the coming weeks."

On January 24, 2022, BIS announced a further request for information concerning methods for strengthening the U.S. semiconductor industry. Secretary of Commerce Gina Raimondo has also urged Congress to pass the United States Innovation and Competition Act of 2021, which includes $52 billion to enhance domestic semiconductor production. Such efforts by Commerce exemplify a whole-of-government approach to identifying and loosening bottlenecks in semiconductor supply chains and increasing U.S. production capabilities.

10. Entity List Designations

As in previous years, BIS continued its liberal use of designations to the Entity List to curtail activities contrary to the national security or foreign policy interests of the United States. As noted above, BIS requires exporters to obtain a license before exporting, reexporting, or transferring specified items subject to the EAR (which, depending on the Entity List designation, can include all items subject to the EAR) to entities appearing on the Entity List. Each such entity is subject to a specific license review policy—most often a presumption of denial. As seen through past designations of such large companies as ***Huawei***, addition to the Entity List can severely restrict a company's access to much-needed goods and can significantly disrupt global supply chains.

Many of BIS's Entity List designations in 2021—as discussed under Section I.B, above—were aimed at countering threats that the United States sees China posing to national security and foreign policy on several fronts. However, the tool was also frequently deployed against actors located beyond the PRC. On March 4, 2021, BIS issued designations for activities in support of Russia's weapons of mass destruction program, followed by additional designations on July 12 for unauthorized support to Russian military programs and on July 19 for unauthorized support to Russian intelligence services. Additionally, on June 1, July 12, and November 26, 2021, BIS announced Entity List designations of entities involved in the proliferation of "unsafeguarded nuclear activities."

BIS also acted to combat cybersecurity threats when, on November 4, 2021, the agency designated two Israeli companies, including ***NSO Group***, for developing and supplying spyware to "foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers" and one Russian entity for "cyber exploits" which threatened the "privacy and security of individuals and organizations worldwide."

In our view, robust use of the Entity List is likely to remain a durable feature of U.S. trade policy, as it has of late become a favored tool across administrations of both political parties to combat a wide range of U.S. national security threats.

B. Antiboycott Developments

Effective June 8, 2021, BIS's Office of Antiboycott Compliance ("OAC") recognized the United Arab Emirates' ("UAE") termination of its participation in the Arab League's boycott of Israel. Part 760 of the EAR and Section 999 of the Internal Revenue Code specifically discourage, and in some circumstances explicitly prohibit, U.S. persons from engaging in activity that would support the Arab League's boycott of Israel, including agreeing to contractual language that directly or indirectly implicates this boycott. OAC's official recognition of the UAE's termination of participation added a new interpretation section to 15 C.F.R. Part 760 which explicitly states that a request from the UAE that an exporter certify that a vessel is eligible to enter UAE ports will no longer carry the presumption that this language was in furtherance of the Arab League's boycott of Israel, and companies can consequently agree to such language as long as no other antiboycott red flags are present. This interpretation comes on the heels of the UAE's normalization of relations with Israel under the Abraham Accords signed on August 16, 2020, and should reduce companies' antiboycott compliance burdens in connection with transactions involving the UAE. We note, however, that sufficient due diligence remains necessary to ensure general compliance with the antiboycott provisions of the EAR. Although BIS does not maintain an official list of boycotting countries, other members of the Arab League (including such countries as Algeria, Iraq, Kuwait, and Saudi Arabia) are widely considered states that frequently include antiboycott restrictions within commercial language.

C. White House Export Controls and Human Rights Initiative

On December 9 and 10, 2021, President Biden convened the first of two Summits for Democracy, which brought together leaders from government, civil society, and the private sector to address threats faced by modern democracies. The virtual summit gathered representatives from over 100 countries and the European Union to address the topics of (1) strengthening democracy and defending against authoritarianism; (2) fighting corruption; and (3) promoting respect for human rights. In connection with the gathering, the United States unveiled its first-ever Strategy on Countering Corruption, which we describe in detail in an earlier client alert.

Notably, the Biden administration used the Summit for Democracy to emphasize its use of export controls to advance human rights. During the Summit, the United States, Australia, Denmark, and Norway jointly announced the Export Controls and Human Rights Initiative, with support from Canada, France, the Netherlands, and the United Kingdom. The initiative aims to create a voluntary code of conduct for states to use in crafting export controls to combat the use of cyber-intrusion and surveillance tools and related technologies by authoritarian governments, both within their countries and across international borders, to track dissidents, censor political opposition, and engage in transnational repression. While WA states have already imposed export controls on tools for military offensive cyber operations and IP network communications systems—the United States announced its own version of the Wassenaar controls on "cybersecurity items" in October 2021—the initiative appears likely to focus

on creating a framework for coordinated unilateral controls on technologies such as biometrics, facial recognition, and other forms of artificial intelligence-assisted surveillance and repression of individuals and ethnic groups.

D. State Department

1. Revisions to ITAR Proscribed Country List

During 2021, the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC"), which administers and enforces the International Traffic in Arms Regulations ("ITAR"), added several new countries to the list of jurisdictions for which the United States prohibits trade in defense articles and defense services. Russia, Ethiopia, and Cambodia were all added to the list of proscribed countries set forth at 22 C.F.R. § 126.1, and the existing entry for Eritrea was updated to codify a broad policy of denial. Accordingly, it is the U.S. Government's policy to deny licenses and other approvals for exports and imports of defense articles and defense services to these countries, except on a case-by-case basis to Cambodia if in furtherance of conventional weapons destruction or humanitarian mine action activities or to Russia if for government space cooperation. Exports of defense articles and services to Ethiopia and Eritrea are only prohibited when destined to or for the armed forces, police, intelligence, or other internal security forces.

2. Revisions to United States Munitions List

DDTC continued to revise the United States Munitions List ("USML") in 2021. Effective August 30, 2021, DDTC extended the temporary modification of Category XI(b) to ensure that certain intelligence-analytics software remained controlled under the USML. This rule extended the temporary revision until August 30, 2026, while DDTC considers a wholesale revision of Category XI. Separately, DDTC was finally able to effect the transfer of software and technical data related to 3-D printing of firearms or components to the EAR, which the State Department first announced in January 2020. This transfer was stayed by a preliminary injunction by the Western District of Washington in March 2020. On May 26, 2021, this injunction was vacated by the Ninth Circuit Court of Appeals, and these items are now exclusively controlled by the EAR. Finally, on September 30, 2021, the State Department extended the temporary modification of the ITAR removing prohibitions on exports, reexports, retransfers, and temporary imports of non-lethal defense articles and defense services destined for or originating in Cyprus. This temporary final rule is effective through September 30, 2022.

3. Changes to Regulations in Light of Remote Work Future

Importantly in a world still significantly impacted by remote working, DDTC has indefinitely authorized "regular employees" to work from remote locations (other than in a country listed in 22 C.F.R. § 126.1) and to send, receive, and access technical data authorized by the U.S. Government for export, reexport, or retransfer to their employer in their country of remote work even if the employer's authorization is for exports to a different country. On May 27, 2021, DDTC solicited comments on the definition of "regular employee" to allow some employees who are contract employees to be treated as regular employees, provided those individuals are sufficiently subject to the employer's control such that the agency can hold the regulated employer responsible for the individual's actions.

V. European Union

A. Sanctions Developments

1. Belarus

2021 saw a major uptick in European Union sanctions, or "restrictive measures," against Belarus. In particular, the EU adopted several rounds of (additional) sanctions packages in response to the Lukashenka regime's human rights violations; violent repression of the opposition; the May 2021 forced landing of a commercial aircraft in Minsk and the resulting arrest of a dissident journalist and his companion; and the instrumentalization of migrants for political purposes.

Of note, the EU Belarus financial sanctions now also target individuals and entities organizing or contributing to activities that facilitate illegal crossing of the EU's external borders, including selected Belarusian travel agencies. Further, the EU, on June 4, 2021, decided to strengthen the existing restrictive measures in view of the situation in Belarus by introducing a ban on the overflight of EU airspace and on access to EU airports by Belarusian carriers of all kinds.

To recall, EU financial sanctions are broadly comparable to U.S. SDN listings. Accordingly, any business dealings with Belarus, specifically any with proximity to the Government of Belarus, but also any travel arrangements for meetings in Belarus or with individuals and entities from Belarus, should undergo additional scrutiny to ensure no funds or economic resources are being made available to those subject to EU financial sanctions.

2. Russia

As tensions between, collectively, the European Union, the United Kingdom, and the United States, and the Russian Federation continue to intensify over a possible impending Russian military intervention in Ukraine, on January 24, 2022, the Council of the European Union (the "Council") issued the Council Conclusions on the European Security Situation. In that document, the Council emphasizes its commitment to the sovereign equality and territorial integrity of states, as well as the inviolability of frontiers and the freedom of states to choose or change their own security arrangements—in this case especially, Ukraine's choice to potentially join NATO. In this context, the Council further elaborates that any further military aggression against Ukraine will have "massive consequences and severe costs," including a wide array of sectoral and individual restrictive measures, in close alignment with the EU's partners. However, the Council does not at this juncture enumerate what specific consequences the EU is prepared to impose. As such, it is challenging to predict the implications for EU sanctions on Russia should the Kremlin launch a further military incursion into Ukraine.

In light of the unstable and fast-developing situation in Ukraine, firms with exposure to Russia may wish to review their existing Russian counterparties to identify possible sanctions targets among their business partners and prepare for the possible imposition of coordinated sanctions by the United States, the United Kingdom, and the European Union. Should Russian troops—thousands of which are presently massed on the border—cross into Ukraine, the wide range of possible sanctions that may be put into effect on a permanent member of the United Nations Security Council likely would be unprecedented and

disruptive. Businesses should therefore consider preparing a contingency plan in the event that sanctions targeting substantial Russian enterprises, including major Russian financial institutions, are issued on short notice.

B. Export Controls Developments

When referring to "EU export controls," we actually refer to a hybrid set of EU and EU member state legislation that together form the export control-related set of rules that apply to parties that undertake business with an EU nexus.

In order to keep up with the latest technological developments and to mitigate national security concerns, the European Union and its member states regularly update its export control regimes. While many of those regular updates cover rather technical aspects, 2021 was different. On September 9, 2021, "Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items (recast)" (the "New EU Dual-Use Regulation") came into effect. The New EU Dual-Use Regulation not only modernizes, but also substantially expands, the scope and breadth of the EU / EU member state system for the control of exports, brokering, technical assistance, transit, and transfer of dual-use products and technologies.

1. Overview

Recasting Council Regulation (EC) No. 428/2009 (the "Old EU Dual-Use Regulation") in its entirety, the New EU Dual-Use Regulation (1) strengthens controls on a wider range of emerging dual-use technologies, including cyber-surveillance tools; (2) specifies due diligence obligations and compliance requirements for exporters, recognizing the role of the private sector in addressing the risks to international security posed by trade in dual-use items; and (3) increases coordination between member states and the European Commission (the "EU Commission") in support of the effective enforcement of controls throughout the EU.

The New EU Dual-Use Regulation is the result of a long period of negotiations between the European Parliament and the Council of the European Union, which started when the reform of EU export controls was initially proposed by the EU Commission in September 2016. Observers have long noted the need for an updated framework due to abundant technological developments, the growing importance of human rights considerations, and growing security risks.

2. Human Rights Considerations

First and foremost, the New EU Dual-Use Regulation specifically includes stronger human rights considerations, resulting in the implementation of stricter controls on exports from the EU of certain surveillance and intrusion technologies that have the potential to contribute to human rights abuses. As Member of the European Parliament Bernd Lange put it, with this update "respect for human rights will become an export standard."

To address the risk that certain cyber-surveillance items exported from EU territory might be misused by persons involved in serious violations of human rights or international humanitarian law, the New EU Dual-Use Regulation now includes a list of such items exceeding international lists in its revised Annex I, making them subject to export control restrictions enforced by the competent authorities of EU member states.

In particular, an authorization may be required even for certain unlisted cyber-surveillance items, if the exporter has been informed by the competent authority that the items in question are or may be intended for use in connection with internal repression and/or committing serious violations of human rights and international humanitarian law. We expect to see increased outreach efforts by the competent authorities of the EU member states in the months to come. In addition, in case an exporter is aware that unlisted cyber-surveillance items proposed for export are or may be intended for human rights violations, exporters are obligated to inform the competent authority.

3. Due Diligence Obligations and Compliance Requirements for Exporters

The New EU Dual-Use Regulation recognizes as vital the contributions of exporters, brokers, providers of technical assistance, and other relevant stakeholders to the overall aim of export controls. As such, the Regulation introduces due diligence obligations and compliance requirements that should be put in place through transaction-screening measures as part of an internal compliance program ("ICP"), which is to be implemented unless the competent national authority of an EU member state considers it unnecessary.

For instance, under the New EU Dual-Use Regulation, exporters using global export authorizations (broadly comparable to U.S. general licenses) should implement an ICP unless the competent national authority considers it unnecessary when processing the application for a global export authorization submitted by the exporter. In that regard, the size and organizational structure of exporters have to be considered when developing and implementing ICPs.

Yet, reporting and specific ICP requirements relating to the use of global export authorizations will be defined by EU member states. The competent authority in Germany has recently done so in published guidance. We assume this guidance will be updated in due course to reflect the New EU Dual-Use Regulation.

In recognition of the importance of sharing research data, academic and industrial research organizations have been included in the new EU regulations and are specifically addressed in Commission Recommendation (EU) 2021/1700, which provides guidance in order to help identify, manage, and mitigate risks associated with the New EU Dual-Use Regulation.

4. Increased Coordination Between EU Member States

To promote a common approach with regard to specific provisions, the New EU Dual-Use Regulation determines that EU member states and the EU Commission should raise awareness and promote tailored guidance to address challenges in the application of this new regime, as well as work together by sharing

information among themselves, especially concerning the technological development of cyber-surveillance items.

5. EU-U.S. Trade and Technology Council

Finally, the New EU Dual-Use Regulation also provides a strong basis for the EU to engage with third countries in order to support a level playing field and enhance international security through more convergent approaches to export controls at the global level.

An example is the U.S.-EU Trade and Technology Council which, as discussed under Section III.E, above, held its inaugural meeting on September 29, 2021. The TTC serves as a forum for both jurisdictions to coordinate approaches to key global trade, economic, and technology issues, as well as to deepen transatlantic trade and economic relations more broadly. The meeting set up various working groups that focus on specific topics including export controls. Additionally, a joint statement was published, stipulating shared principles and areas for export cooperation. The TTC recognizes, among other things, the importance of a multilateral approach to export controls and lays a focus on dual-use items as such may be misused for violations of human rights. These areas of cooperation may also suggest that the European Union and the United States plan to use the TTC to further communicate and potentially synchronize their efforts on export controls as part of a joint approach to trade with China.

Under the New EU Dual-Use Regulation, companies will be burdened with the additional task to support the EU's endeavor to protect and secure human rights. As a major amendment, companies will, even more so than before, be well advised to screen their transactions for possible dual-use technology, now including cyber-surveillance tools that could be used to violate human rights. Which specific standards will need to be applied to comply with such due diligence and ICP obligation remains to be seen, as such standards are currently being finally determined by the EU and its EU member states.

C. Noteworthy Judgments and Enforcement Actions

1. EU Blocking Statute Regulation

Following Advocate General Gerard Hogan's Opinion of May 12, 2021, the European Court of Justice ("ECJ") on December 21, 2021 delivered its highly anticipated decision in *Bank Melli Iran, Aktiengesellschaft nach iranischem Recht v. Telekom Deutschland GmbH* (C-124/20), involving interpretation of Council Regulation (EC) No 2271/96 (the "Blocking Statute Regulation").

In its judgment—which adds to the growing body of case law concerning the circumstances under which parties can be judicially compelled to comply with the Blocking Statute Regulation—the ECJ provided guidance on three questions brought before the court:

First, the Blocking Statute Regulation impedes a contractual party from unilaterally terminating a contract with another party that is subject to U.S. "secondary" sanctions because the terminating party seeks to comply with such U.S. sanctions. This principle applies even without any prior compelling request by the U.S. administration for compliance with U.S. sanctions.

Second, under the Blocking Statute Regulation, a party that wishes to terminate a contract with a person subject to U.S. sanctions is not per se obliged to put forward a reason for such termination. However, if the termination is subject to proceedings before an EU member state court, the terminating party will have the burden of proof to demonstrate that such termination was not induced by compliance with the U.S. sanctions listed in the Blocking Statute Regulation if the evidence available to the national court suggests *prima facie* that the terminating party in fact complied with U.S. sanctions.

Third, the ECJ ruled that, in principle, the annulment of a termination by a national court shall be compatible with the fundamental right of freedom to conduct a business (Article 16 of the Charter of Fundamental Rights of the European Union ("CFR")) and the principle of proportionality (Article 52 CFR) if the national court concluded that the notice of termination was given for the purpose of compliance with certain specified U.S. sanctions.

However, the ECJ also held that it is ultimately up to the national court to determine whether further performance of the contract could lead to disproportionate economic or financial consequences for the terminating party. In this regard, it is important to note that the ECJ stressed that one of the factors to take into consideration is whether or not the terminating entity applied for an exemption from the Blocking Statute Regulation prior to termination.

In addition, more on a side note, the ECJ gives its opinion on the Guidance Note to the Blocking Statute issued by the European Commission, stating that the document does not establish binding rules or interpretations. The ECJ further notes that only the Blocking Statute Regulation is binding and only the ECJ has the power to provide legally binding interpretations of that regulation. Although we believe the Guidance Note still provides some valuable guidance for the *de facto* interpretation of the Statue, its persuasive power in court is likely to be greatly reduced.

2. Denmark

On December 14, 2021, the Court of Odense sentenced Danish fuel supplier ***A/S Dan-Bunkering Ltd.*** and its parent company ***Bunker Holdings A/S*** to payments of 45 million Danish Crowns ($6.9 million) and 4 million Danish Crowns ($600,000) for violating EU sanctions. The holding company's chief executive officer has also been sentenced to a suspended prison sentence of four months.

The court found that Dan-Bunkering, via its Kaliningrad office, purposely violated EU Regulation No. 36/2012 of 18 January 2012, as amended, which implemented restrictive measures against Syria. Dan-Bunkering had sold 172,000 tons of jet fuel worth over $100 million through a total of 33 trades between October 2015 and May 2017. The deals were made with two Russian companies listed on the U.S. sanctions list that ultimately acted as agents for the Russian Navy. The traded jet fuel was later used to execute Russian bombing runs near the Syrian city of Banias. The fines set by the court's judgment ultimately are equivalent to double the profit Dan-Bunkering achieved from the deals. The court ruled that Dan-Bunkering must have been aware of a possible usage of their products for Russian interference in the Syrian war.

Notably, the verdict affirms that EU courts do not hesitate to hold business managers personally accountable for their company's breach of sanctions. The decision also highlights the importance of maintaining an effective sanctions compliance program.

3. Germany

In 2021, the German Federal Court of Justice (*Bundesgerichtshof*) ("BGH") dealt with multiple cases regarding payments made to members of the Islamic State. In the context of these judgments, the court clarified its interpretation of the scope of "mak[ing] available, directly or indirectly, to, or for the benefit of, a natural or legal person, group or entity designated" under Article 2.II of Regulation (EC) No. 881/2002.

The main focus of these cases was whether a private benefit to an individual is also "made available" to an organization of which that individual is a member or with which that individual is associated. The BGH used the rulings to emphasize that the wording at issue should be interpreted broadly. While the court leaves open the possibility that payments could be made to individuals regardless of their affiliation with organizations on the sanctions list, it sets a high bar for such defense. Any kind of economic benefit to the organization results in the good or service being considered as "made available" to the organization. In this context, it is also deemed irrelevant whether the service is provided in direct exchange for a service in return.

These rulings develop their practical relevance in that they shed light on how much distance should be maintained from organizations and persons appearing on the EU sanctions list in order to avoid running afoul of EU sanctions.

VI. United Kingdom

A. Sanctions Developments

Following the end of the Brexit transition period on December 31, 2020, the United Kingdom is no longer bound by EU sanctions law. The Sanctions and Anti-Money Laundering Act 2018 (the "Sanctions Act") now provides the legislative framework for the UK's post-Brexit sanctions regime. The year of 2021 constitutes the first full year that the UK's autonomous sanctions regime has been underway.

1. OFSI Annual Review 2020-2021

On October 14, 2021, the UK Office of Financial Sanctions Implementation ("OFSI") published its annual review for the financial year April 2020 to March 2021 (the "OFSI Annual Review"). The OFSI Annual Review comments on the impact of the end of the Brexit transition period on its activity levels, stating that "OFSI has had a stretching year, working across government and with both private sector and international partners as it transitioned out of the EU and into a UK autonomous sanctions framework." Other key takeaways of the OFSI Annual Review include:

- Changes to the Consolidated List: OFSI added 278 new designated persons to the consolidated list in the financial year 2020 to 2021, 159 of which implemented EU and UN legislation, outside of the period before the end of the Brexit transition period on December 31, 2020. Furthermore, 119 designations were made under the new Sanctions Act.

- Licensing: The OFSI Annual Review highlights how the transition to an autonomous sanctions framework led to changes to licensing, including new licensing grounds (derogations) in respect of non-UN designated persons and adjustments to existing licensing grounds. For example, the existing licensing grounds for "maintenance of frozen funds and economic resources" and for payment of legal fees and expenses now require "reasonableness." Under the Sanctions Act, OFSI was also granted new powers to provide for issuing General Licences under all regimes; previously, it could only issue these under the Terrorist Asset-Freezing etc. Act 2010. A General License allows multiple parties to undertake specified activities that would otherwise be prohibited without the need for a specific licence. In the financial year 2020 to 2021, OFSI issued 43 new licenses and made 75 amendments across 11 regimes; 64 out of the 75 amendments to licenses issued were issued under the Libya regime.

- Compliance and Enforcement: The OFSI Annual Review makes clear that OFSI investigates every reported suspected breach of UK sanctions regulations, the result of which can vary depending on whether a breach has occurred and, if so, the nature of the breach. Where a breach has occurred, proportionate action can include the issuance of a warning letter, a civil monetary penalty, or escalation to law enforcement partners. In the financial year 2020 to 2021, OFSI considered 132 reports of potential financial sanctions breaches. This is a slight decrease from the previous financial year; however, generally the number of cases considered remains on an upwards trajectory from earlier years.

2. Sanctions Regulations Report on Annual Reviews 2021

The Sanctions Regulations Report on Annual Reviews 2021 has been published by the UK Foreign, Commonwealth & Development Office (the "Report"). The review is required under Section 30 of the Sanctions and Anti Money Laundering Act 2018, to assess whether the regulations are still appropriate for the purpose for which they were created. The report summarizes and reviews activity under the UK's sanctions policy during 2021. The Report highlights the fact that the UK has become "more agile and has real autonomy to decide how [it] use[s] sanctions and where it is in our interests to do so" since leaving the EU and moving to an independent sanctions policy.

The Report observes the value of this in two recently established UK autonomous sanctions regimes: (1) the launch of the Global Human Rights sanctions regime on July 6, 2020; and (2) the launch of the Global Anti-Corruption sanctions regime on April 26, 2021. At the time of the Report, 106 designations have been made under these two regimes, "ensuring and sending a clear message that the UK is not a safe haven for those individuals and entities involved in serious corruption and human rights violations or abuses, including those who profit from such activities."

3. Changes to Sanctions Lists

OFSI announced in December 2021 that, with effect from February 2022, the structure and data fields included in the UK sanctions list and the OFSI consolidated list will be changing.

The key changes to the UK sanctions list include the standardization of data (where possible) to remove duplications, unnecessary punctuation, and improve consistency; the creation of new fields to improve the detail and structure of the data; and changes to some field names to make their purpose clearer.

The key changes to the OFSI sanctions list include the addition of seven new fields, the introduction of a new group type "Ship," and the retirement of the .xls format.

Organizations that regularly use the UK sanctions list and OFSI consolidated list in order to conduct sanctions checks should ensure that they understand these changes with a view to updating their systems, processes, and compliance policies accordingly.

B. Export Controls Developments

The UK's status in relation to the EU has changed following the end of the Brexit transition period on December 31, 2020. Though the UK regime has similarities to the New EU Dual-Use Regulation, it now has its own sanctions and export control regimes, separate from those of the EU. In light of these changes, the UK Government published guidance on exporting military or dual-use technology (the "UK Guidance").

1. Overview

In the UK export regime, "dual-use" means useable for both civil and military purposes. This includes dual-use goods, along with software or technology. In contrast to the human rights rhetoric used in describing the New EU Dual-Use Regulation, the UK dual-use export controls focus primarily on national security. The UK Guidance describes the basis of the UK's export controls as aimed at preventing transfers that can lead to goods causing national security concerns for the UK and its allied forces, but doing so without "inhibiting legitimate trade [and] knowledge acquisition."

Though the fines for dual-use export control violations pre-Brexit have been relatively low in the UK, with fines for export control violations in 2020 amounting to GBP 700,368 in total, the position post-Brexit and in light of the UK Guidance remains unclear.

2. Open Export General License

Broadly speaking, the EU and UK have sought to keep their respective post-Brexit trade control regimes aligned to minimize disruption to the pre-Brexit status quo. While the main features of the EU dual-use regime are seen in the UK regime, they are applied in the UK as a matter of English law rather than EU law. As such, when developing and implementing ICPs, the UK should be considered separately from the EU.

Furthermore, as the UK is no longer a member of the EU, the UK is now treated as a "third country" with respect to the EU's export controls. This means that whereas previously most exports of dual-use

items between the UK and EU member states did not require licenses, now exports from the UK to EU member states of dual-use goods or technology will require export authorization by way of an Open General Export License (an "OGEL").

This new requirement, along with the heightened focus on technology, will not only impact companies that export dual-use goods, but also will have a bearing on how a company will transfer its "controlled technology" (i.e., information necessary to develop, produce, or use goods or software subject to UK dual-use export controls) within its international offices or employees, along with how such information is stored and accessed remotely (i.e., cloud storage).

3. Guidance on Exporting Military or Dual-Use Technology

The UK Guidance provides clarification regarding UK dual-use export controls including their applicability and scope, confirming that UK dual-use export controls apply to any entity in the UK and, in some circumstances, UK persons overseas.

In particular, the UK Guidance confirms that an OGEL for dual-use items will now be required for the transfer of controlled technology. A "transfer" includes sharing information via phone or video conferencing, emails, or laptops, phone or memory devices. Transfers can also include where the information is read out loud, shared via screensharing presentations, sent via email, or taken overseas on a memory device. Given the rise in remote working and the increased usage of video conferencing services, companies will need to be conscious of what information and data is shared overseas from their UK bases, and whether an OGEL will be required.

The Guidance also addresses the storage of controlled technology on servers that can be accessed remotely. It confirms that the location of the exporter and intended recipient, and not the location of the servers containing the controlled technologies themselves, will determine the need for an OGEL. As such, an OGEL is required if controlled technology is uploaded by persons in the UK and subsequently accessed by a recipient overseas.

This is of particular importance to multinational companies that transfer and store controlled technology through common IT systems and utilize intranets or cloud services. Companies falling into this category will now require an OGEL in order to share controlled technology from within the UK to their overseas offices, regardless of where that information is subsequently stored.

4. Updates to the Export Control Regime

On December 8, 2021, an update on the UK export control regime was released by the Secretary of State for International Trade, comprising three new measures.

Firstly, the UK Strategic Export Licensing Criteria have been amended, which will be applied with immediate effect to all license decisions on goods, software, and technology which are subject to control for strategic reasons for export, transfer, trade, and transit. For example, they lay a stronger focus on risks of violation of humanitarian law and misuse of items for internal repression, similar to the New EU Dual-Use Regulation.

In addition, a broader definition of military end-use will be established in early 2022, which will now permit control (on a case-by-case basis) of non-listed items intended for use by military and other security forces, apart from the previously covered listed items. However, the control will only be imposed when the government informs the exporter that a proposed export is intended for a military end use. To minimize the impact on legitimate trade, there will be exemptions for medical supplies and equipment, food, clothing, and other consumer goods.

Last but not least, China is expected to be added to the list of destinations subject to military end-use controls by spring 2022.

C. Noteworthy Judgments and Enforcement Actions

On August 5, 2021, OFSI announced a GBP 50,000 monetary penalty against the UK fintech company ***TransferGo Limited*** ("TransferGo") for multiple breaches of The Ukraine (European Union Financial Sanctions) (No. 2) Regulations 2014. As stated in OFSI's penalty report, the penalty related to 16 transactions made between March 2018 and December 2019, where TransferGo issued instructions to make payments to accounts held at the ***Russian National Commercial Bank*** ("RNCB"), a designated party under Council Regulation (EU) No 269/2014. The total value of the transactions was GBP 7,764.77.

OFSI imposed a monetary penalty because it was satisfied, on the balance of probabilities, that TransferGo breached a prohibition imposed by financial sanctions legislation and either knew or had reasonable cause to suspect that it was in breach of that prohibition. OFSI further elaborated that TransferGo erred in its assessment of whether the payments to RNCB were subject to financial sanctions restrictions. TransferGo asserted that payments to the accounts with RNCB were not breaches of financial sanctions restrictions since the relevant clients and beneficiaries were not themselves subject to such restrictions. However, OFSI considered that funds held in bank accounts ultimately belong to those banks.

VII. People's Republic of China

China continued building up its legal arsenal against the continuing pressure from the United States. As we reported in our 2020 Year-End Sanctions and Export Controls Update, China had already begun establishing a sanctions blocking law and an export controls system. However, the myriad PRC policy developments that took place in 2021 extended even more broadly to include blocking laws and counter-sanctions, export controls, data security laws, national security reviews of foreign investments, and cybersecurity reviews. Importantly, these measures appear to be a symbolic statement against the United States and its allies that China will not back down in the strategic competition between Washington and Beijing. These measures also appear to be part of China's efforts to build a resilient economic and business ecosystem and further establish itself as a major power in setting alternative global norms and standards.

The ink on these measures is barely dry and, because these measures were written in broad strokes and afford considerable discretion to PRC regulators, the compliance implications for global businesses are not yet clear. However, one certainty is that the new measures unveiled by PRC authorities have already

increased the complexity and risk of doing business globally, especially when taken together with the various U.S. policy changes discussed above, such as heightened supply chain due diligence expectations and the ever-growing list of sanctioned Chinese entities. Global businesses with operations touching China now must monitor the developments in not only the U.S. legal regimes targeting China, but also the increasingly intricate set of Chinese legal rules.

A. Countermeasures on Foreign Sanctions

As the United States continued to impose a litany of trade restrictions on China in 2021, China showed few signs of backing down. In January and June 2021, China issued a set of laws that would allow the Chinese government to prohibit compliance with certain foreign laws. These laws could potentially require companies active in the global supply chain to choose whether to comply with U.S. sanctions or to comply with Chinese law. Although the practical impact of these developments is yet unclear, we are already seeing Chinese companies balk at agreeing to traditional representations and warranties in agreements, which may compel Western firms to reconsider how to obtain assurances regarding sanctions compliance going forward. Using its new legal tools, China has also counter-sanctioned several U.S. and other Western officials and entities in response to sanctions related to Xinjiang and Hong Kong. This cycle of sanctions and counter-sanctions appears likely to proliferate so long as relations between the United States and China remain fraught and the two superpowers continue their competition for global primacy.

1. Blocking Rules

As discussed in an earlier client alert, the Chinese Ministry of Commerce ("MOFCOM") on January 9, 2021 issued the Rules on Blocking Unjustified Extraterritorial Application of Foreign Legislation and Other Measures (the "Blocking Rules"), which took immediate effect. (The Blocking Rules are available in both a Chinese-language version and an English translation.) The Blocking Rules established a mechanism for the Chinese government to designate "unjustified extraterritorial applications of foreign legislation and other measures" and issue prohibitions on Chinese persons' and entities' compliance with these foreign laws (Articles 4 & 7). Whether a foreign law constitutes "unjustified extraterritorial applications" is determined on an open-ended set of factors, including whether the law violates "international law or the basic principles of international relations," impacts China's "national sovereignty, security and development interests," or impacts the "legitimate rights and interests" of Chinese individuals and entities, as well as a catch-all for "other factors that should be taken into account" (Article 6).

Under the Blocking Rules, Chinese individuals and entities—including, critically, Chinese subsidiaries of multinational companies—must report any restrictions they face from foreign governments (Article 5). Failure to comply may result in government warnings, orders to rectify, or fines (Article 13). Chinese individuals and entities also have a private right of action to sue in Chinese courts for compensation from any restrictions (Article 9). If carried out effectively, the Blocking Rules have the potential to create significant compliance risks for multinational enterprises.

Although the Blocking Rules went into effect immediately, they will only become enforceable in substance once the Chinese government designates the specific "unjustified extraterritorial applications"—a step that, as of this writing, has not yet been taken. Nevertheless, the Blocking Rules by their publication have forcefully communicated the Chinese government's intention to establish a legal regime for countering foreign sanctions.

2. Anti-Foreign Sanctions Law

On June 10, 2021, the National People's Congress further bolstered the message by passing the Law of the People's Republic of China on Countering Foreign Sanctions (the "Anti-Foreign Sanctions Law"), which took immediate effect. (The Anti-Foreign Sanctions Law is available in both a Chinese-language version and an English translation.) The legislation formalizes previous administrative measures taken by China, such as the Blocking Rules and the Export Control Law (discussed below), by providing legal grounds for the countermeasures. Coming one day before the start of the G7 summit in the United Kingdom, the legislation was widely believed to be, at least in part, China's challenge to President Biden's objective at the G7 to build a coalition against China's rising global influence.

Importantly, the Anti-Foreign Sanctions Law allows Chinese authorities to designate on the "Countermeasures List" and take a menu of counter-sanctions—including denial of visas, seizure of assets, blocking of transactions, and other necessary measures—against individuals (as well as their spouses and immediate relatives) or entities (as well as their senior management and controllers) involved in creating, deciding, or implementing "discriminatory restrictive measures" by foreign governments (Articles 4 to 6). The term "discriminatory restrictive measure" is left undefined—but it is likely to include China-related sanctions and export controls by foreign governments.

In announcing the Anti-Foreign Sanctions Law, China hinted that enforcement of this legislation may be limited to those involved in drafting and advocating for sanctions targeting China as "[t]he law only takes aim at those entities and individuals who grossly interfere in China's internal affairs and spread rumors about and smear, contain and suppress China." That said, like the Blocking Rules, the Anti-Foreign Sanctions Law also prohibits Chinese persons and entities from complying with foreign "discriminatory restrictive measures" and allows a private right of action for Chinese persons and entities that are negatively impacted by sanctions to seek injunctive relief and compensatory damages (Article 12). Even if the Countermeasures List designations may be reserved for those closer to the formulation of U.S. sanctions measures, private companies seeking to comply with U.S. sanctions must now carefully navigate between the conflicting regulatory requirements of the world's two largest economies.

3. Impact on Entities in Hong Kong

Even before the introduction of the measures described above, multinational businesses and financial institutions in Hong Kong were faced with a dilemma. The Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region (the "National Security Law"), which has been in effect in Hong Kong since June 30, 2020, established the crimes of secession, subversion, terrorist activities, and collusion with a foreign country or external elements to

endanger national security. At the time of the National Security Law's enactment, about 54 percent of businesses in a Hong Kong General Chamber of Commerce survey expressed concern about potential foreign sanctions risks—albeit in the short term—arising from the National Security Law.

On August 8, 2020, the Hong Kong Monetary Authority issued guidance instructing regulated institutions that "unilateral sanctions imposed by foreign governments are not part of the international targeted financial sanctions regime and have no legal status in Hong Kong." However, the guidance did not expressly prohibit companies from complying with U.S. sanctions and instead advised that companies' policies should be "informed by a thorough assessment of any legal, business and commercial risks involved and based on a balanced approach. In assessing whether to continue to provide banking services to an individual or entity designated under a unilateral sanction which does not create an obligation under Hong Kong law, boards and senior management of [regulated institutions] should have particular regard to the 'treat customers fairly' principles."

Naturally, the enactment of the Anti-Foreign Sanctions Law again created a quagmire for Western businesses and financial institutions in Hong Kong. At the same time, however, China seems to be treading lightly to avoid discouraging foreign business activities in Hong Kong. In the August 2021 session, the National People's Congress postponed a vote on extending the Anti-Foreign Sanctions Law to Hong Kong. On October 5, 2021, Hong Kong Chief Executive Carrie Lam provided some comfort to businesses by further clarifying that Beijing has shelved the extension of the Anti-Foreign Sanctions Law to Hong Kong and would take into account Hong Kong's status as an international financial center even if the extension were to occur in the future.

4. Application of Counter-Sanctions

In part aided by the new legal regimes, the Chinese Ministry of Foreign Affairs ("MOFA") issued counter-sanctions against major Western decisionmakers throughout the year. From March 22-27, 2021, MOFA announced counter-sanctions against 22 individuals and ten entities from the European Union, the United Kingdom, and the United States and Canada "in response" to sanctions imposed days earlier for alleged human rights abuses in Xinjiang. On July 23, 2021, MOFA announced a further round of counter-sanctions against seven individuals and one entity in the United States (including former Commerce Secretary Wilbur Ross) in response to the sanctions imposed on Chinese officials in connection with repression of protests in Hong Kong. On December 21, 2021, MOFA announced additional counter-sanctions against four members of the U.S. Commission on International Religious Freedom shortly after the United States imposed sanctions and announced a diplomatic boycott of the 2022 Beijing Winter Olympics related to the situation in Xinjiang. Although Chinese counter-sanctions have to date principally focused on Western government officials and agencies, such measures have also targeted scholars and non-profit organizations known for their advocacy of human rights.

Such tit-for-tat sanctions are likely to continue. Despite the November 2021 virtual meeting between President Biden and President Xi in which the two leaders discussed "the importance of managing competition responsibly," the U.S.-China relationship remains tense. As the United States continues to impose sanctions and other policy measures targeting China, China may not simply let its newest policy tool gather dust.

B. Export Controls Regime

China's first comprehensive Export Control Law (Chinese version here and English translation here), which went into effect on December 1, 2020, included a notable expansion of extraterritorial applicability, as we previously reported in an August 2020 client alert. In the intervening months, China has issued a number of regulations in relation to export controls, especially for dual-use items (i.e., items with both civil and military applications). For example, China announced new rules on commercial cryptographic products, updated the catalog of dual-use items and technologies subject to import and export license administration, and implemented paperless management of import and export licenses for dual-use items and technologies. While not a "sea change" per se, these regulations are evidence of China's ongoing efforts to solidify and modernize its export controls regime.

On April 28, 2021, MOFCOM issued Guiding Opinions on Establishing the Internal Compliance Mechanism for Export Control by Export Operators of Dual-Use Items (the "Guiding Opinions"), answering the Export Control Law's call for official internal compliance guidelines. The Guiding Opinions' core elements of a sound internal compliance mechanism largely parallel those found in the U.S. Export Compliance Guidelines, thus allowing global companies to maintain consistency in their global compliance programs. The core elements of the Chinese Guiding Opinions include, among others: (1) issuing a statement of policy (equivalent to the "management commitment" in the U.S. Export Compliance Guidelines); (2) assigning a department and personnel responsible for export controls compliance; (3) conducting a comprehensive risk assessment; (4) establishing a set of internal controls to screen for red flags; and (5) conducting periodic compliance audits.

C. Restrictions on Cross-Border Transfers of Data

Prior to 2021, China already maintained several restrictions on the provision of data to foreign governments. For example, the International Criminal Judicial Assistance Law (Chinese version here and English translation here) bars Chinese individuals and entities from providing foreign enforcement authorities with evidence, materials, or assistance in connection with criminal cases without the consent of the Chinese government, and the China Securities Law (Chinese version here and English translation here) prohibits "foreign regulators from directly conducting investigations and collecting evidence" in China. In 2021, China issued the Data Security Law and the Personal Information Protection Law, thereby clamping down on the sharing of broader swaths of personal and corporate data outside its borders. With these recent developments, the restrictions now also apply in the context of civil enforcement actions and litigation, as well as general corporate practices including due diligence. Coupled with the blocking measures discussed above, these data restrictions could have a far-reaching impact on multinational companies.

1. Data Security Law

On the same day in June 2021 that China's Anti-Foreign Sanctions Law was passed, the National People's Congress also passed the Data Security Law (Chinese version here and English translation here), which took effect on September 1, 2021. As described in our June 2021 client alert, the legislation contains sweeping requirements and severe penalties for violations. It governs not only data processing

and management activities within China, but also those outside of China that "damage national security, public interest, or the legitimate interests of [China's] citizens and organizations."

The Data Security Law generally creates strict data localization and data transfer requirements for entities and individuals operating within China, depending upon the category of data (e.g., "core data" or "important data"). Crucially, the Data Security Law prohibits the provision of *any* "data stored within the People's Republic of China to foreign judicial or law enforcement bodies without the approval of the competent authority of the People's Republic of China" (Article 36). Failure to obtain this prior approval may result in significant fines and, in some "serious" cases, suspension of business operations and revocation of business licenses (Article 48). The need to seek prior approval for any cross-border transfer of data creates substantial barriers to responding to government enforcement actions and lawsuits.

The Data Security Law also authorizes the Chinese government to implement "equal countermeasures" when a foreign country enacts any "discriminatory, restrictive, or other similar measures" with respect to investment or trade related to data and technology for data development and utilization (Articles 26). This provision appears to be a reference to recent U.S. sanctions and export controls targeting China's technology sector and provides the Chinese government another sanctions tool under the data security regime.

The Data Security Law, like other PRC measures discussed above, leaves certain important terms undefined. In our experience, it is likely that the PRC authorities will issue additional guidance and implementation rules that provide further clarity, similar to the Provisions on the Management of Automobile Data Security that were issued on August 16, 2021 and which provide some insight into the definition of "important data" in the context of the automobile industry.

2. Personal Information Protection Law

On August 20, 2021, the National People's Congress further built out the data protection regime when it passed the Personal Information Protection Law (Chinese version here and English translation here), which took effect on November 1, 2021. As described more fully in our September 2021 client alert, the legislation asserts an extensive extraterritorial reach. It governs not only domestic companies, but also foreign companies that process or use the personal information of individuals located within China for the purpose of providing products or services to individuals in China, analyzing or assessing the behavior of individuals in China, or under other unspecified circumstances provided in laws or regulations (Article 3). Foreign companies without a physical presence in China must appoint a designated representative in China for personal information protection (Article 53).

The Personal Information Protection Law generally requires personal information processing entities to adopt certain protective measures. Processing entities are only allowed to transfer personal information overseas if they: (1) pass a security assessment administered by the Cyberspace Administration of China ("CAC"); (2) obtain a certification from professional institutions in accordance with the rules of the CAC; (3) enter into a transfer agreement with the transferee using the standard contract published by the CAC; or (4) adhere to other conditions set forth by law, administrative regulations, or the CAC, unless

any relevant international treaties to which China is a party stipulate otherwise (Article 38). Violations of the law's requirements may lead regulators to take corrective actions, issue warnings, confiscate unlawful income, suspend services, revoke operating permits or business licenses, and/or issue fines (Article 66). Moreover, individuals may bring civil tort claims if the processing entities infringe their rights and interests (Article 69), and the People's Procuratorate may file public interest lawsuits if the rights and interests of a large number of individuals are affected (Article 70).

Similar to the Data Security Law, the Personal Information Protection Law allows the Chinese government to take "reciprocal measures" if any country or region takes "discriminatory prohibitions, limitations, or other similar measures" against China in the area of personal information protection (Article 43). At the same time, the Personal Information Protection Law suggests a commitment by the Chinese government to "participate[] in the formulation of international rules for personal information protection, stimulate[] international exchange and cooperation in personal information protection, and promote[] mutual recognition of personal information protection rules and standards with other countries, regions, and international organizations" (Article 12). This language reinforces the notion that Beijing may be interested in challenging the Western powers by promoting an alternative "model" of global norms and standards.

D. Security Review of Foreign Investments

Finally, any discussion of China's growing arsenal of trade controls would be incomplete without a least a brief mention of China's foreign investment review regime. The Foreign Investment Law took effect on January 1, 2020, focusing on foreign investment promotion, protection, and administration, and also noting that China will establish a system for the security review of foreign investments. Shortly after the anniversary of the Foreign Investment Law, in January 2021, the rules for this new security review system went into effect. Additionally, in December 2021, the rules for the new cybersecurity review were also announced in connection with the Data Security Law described above.

1. National Security Review

On December 19, 2020, China's National Development and Reform Commission ("NDRC") and MOFCOM issued the Measures for Security Review of Foreign Investment (the "Security Review Measures") (Chinese version here and English translation here) which apply to investments closed after January 18, 2021. Prior to the new Security Review Measures, national security review of foreign investment was set forth under circulars issued by the State Council in 2011 and 2015. In addition to formalizing the existing national security review regime, the Security Review Measures made important changes to its scope and process.

The Security Review Measures substantially expand the scope of foreign investment subject to national security review. First, the national security review now captures not only direct foreign investments, but also indirect foreign investments—which include an offshore transaction between two foreign parties in which a foreign investor acquires indirect "actual control" (whether by way of 50 percent ownership or through other decision-making powers) of a Chinese target. Second, the national security review not

only covers an investment in or acquisition of equities or assets in China, but also the establishment of new enterprises, such as subsidiaries or joint ventures (also known as "greenfield investments").

The Security Review Measures create a mandatory review requirement by a new Working Office that is jointly headed by the NDRC and MOFCOM if:

- The investment is (i) in sectors related to national defense and security, or (ii) in geographic locations in close proximity to military facilities or defense-related industries facilities; or

- The investment (i) involves important sectors significant for national security, such as agricultural products, energy and resources, equipment manufacturing, infrastructure facilities, transportation services, cultural products and services, information technology and internet products and services, financial services, and key technologies, and (ii) will result in foreign investors' actual control.

Because the sectors listed above cover a broad range and are not specifically defined, the Security Review Measures potentially create a widely-applicable mandatory pre-closing filing requirement—a key difference from the U.S. CFIUS review mechanism, which is a largely voluntary process. If a party fails to submit a mandatory application, the Working Office may require the submission of an application. If the parties still fail to submit an application, the Working Office may reverse the transaction through a divestment order or other actions. This, in theory, creates a significant risk for foreign investors considering an investment involving a Chinese interest in a sensitive industry. It remains to be seen, however, how aggressively China will enforce these measures as it vows to continue opening up to foreign investments.

2. Cybersecurity Review

On July 2, 2021, the CAC launched an investigation into ***DiDi Global Inc.'s ("DiDi")*** June 30 initial public offering ("IPO") on the New York Stock Exchange, marking the first cybersecurity review based on the measures implemented in June 2020. The CAC expressed concerns regarding the company's network security practices and required the company to remove its app from local app stores, thus suspending any new-user registration, during the review period. On July 5, 2021, the CAC further expanded the investigation into ***Full Truck Alliance*** and ***Kanzhun***, which had also recently listed in the United States.

On July 10, 2021, the CAC released a draft revision to the existing Cybersecurity Review Measures. The final measures were issued on December 28, 2021 (Chinese version here and English translation here), and will go into effect on February 15, 2022. The Cybersecurity Review Measures capture not only critical information infrastructure operators but also data processing activities by internet platform operators (Article 2), and expand the regulatory and enforcement agencies to include the China Securities Regulatory Commission ("CSRC") (Article 4). Importantly, the Cybersecurity Review Measures require operators that hold personal information of more than one million users to report for a cybersecurity review by the CAC before going public on stock exchanges outside China (Article 6). The report to the CAC must include IPO materials prepared for submission (Article 8). Finally, the Cybersecurity Review Measures extend the "special review" period for a typical case from 45 working

days to 90 working days (Article 14)—potentially causing significant delays to foreign listing preparation schedules.

These reviews can cause significant disruption. For example, on December 3, 2021, DiDi eventually announced that it would de-list from the New York Stock Exchange, following a five-month investigation. Amidst market turmoil from the series of investigations, the CSRC assured foreign investors that China has always supported Chinese companies choosing listing destinations of their own. However, uncertainties linger for Chinese companies listed in the United States, especially after the December 2020 enactment of the Holding Foreign Companies Accountable Act and the December 2021 adoption by the U.S. Securities and Exchange Commission of its final rule implementing this legislation, which would authorize the de-listing of Chinese firms unless they abide by U.S. accounting and auditing requirements. This, of course, requires careful balancing with the Data Security Law and the Personal Information Protection Law, both discussed above. Thus, foreign investors who have already invested or plan to make investments in China or Chinese companies should closely monitor the changing legislative landscape with respect to data security.

The following Gibson Dunn lawyers assisted in preparing this client update: Scott Toussaint, Richard Roeder, Judith Alison Lee, Adam M. Smith, Patrick Doris, Michael Walther, Attila Borsos, Fang Xue, Qi Yue, Christopher Timura, Sean Brennan, Laura Cole, Kanchana Harendran, Nicole Lee, Chris Mullen, Rose Naing, Sarah Pongrace, Cody Poplin, Anna Searcey, Samantha Sewall, Audi Syarief, Lindsay Bernsen Wardlaw, Xuechun Wen, Brian Williamson, and Claire Yi.

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)
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)
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)
Chris R. Mullen – Washington, D.C. (+1 202-955-8250, cmullen@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:
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)