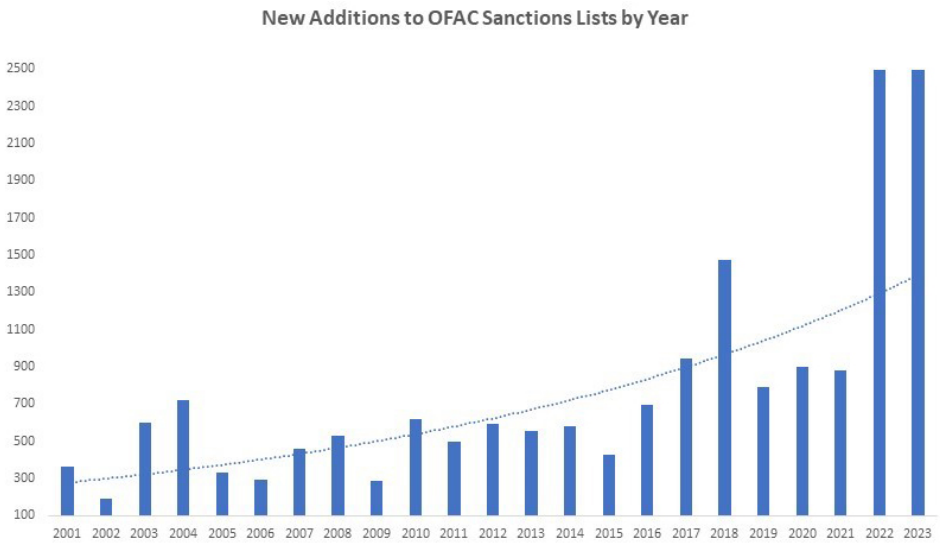
GIBSON DUNN

2023 Year-End Sanctions and Export Controls Update

Client Alert | February 7, 2024

2023 was another extraordinarily active year in the world of trade controls, including sweeping new trade restrictions on Russia and China, aggressive enforcement of sanctions and export controls, and extensive collaboration among sister agencies and partner countries.

In 2023, the United States, the European Union, and the United Kingdom continued to push the limits of economic statecraft by imposing new trade restrictions on major economies such as Russia and China, and aggressively enforcing existing measures. Throughout his tenure, President Biden has imposed sanctions at an unprecedented rate by adding nearly 5,500 names to restricted party lists maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC")—a yearly average nearly double that of the Trump administration and triple the pace under President Obama. Approximately one-third of all parties presently on U.S. sanctions lists were placed there by President Biden. That sharp upswing continued in 2023 as the United States added a near-record number of individuals and entities to OFAC sanctions lists:



In addition to the sheer number of new sanctions designations, the past year was noteworthy for the scale and scope of enforcement actions targeting sanctions and export control violations. OFAC and the U.S. Department of Commerce's Bureau of Industry and Security ("BIS") each issued record-breaking civil monetary penalties measured in the hundreds of millions of dollars and closely coordinated with the U.S. Department of Justice to mount criminal prosecutions—marking a historically aggressive approach to enforcing trade controls.

Indeed, a high degree of collaboration among sister agencies and partner countries was

Related People

Scott R. Toussaint

Irene Polieri

Adam M. Smith

Stephenie Gosnell Handler

Christopher T. Timura

Michelle M. Kirschner

Benno Schwarz

Attila Borsos

David A. Wolber

Amanda H. Neely

Dharak Bhavsar

Erika Suh Holmberg

Zach Kosbie

Allison Lewis

Nikita Malevanny

Chris R. Mullen

Sarah L. Pongrace

Anna Searcey

Samantha Sewall

Dominic J. Solari

Audi K. Syarief

Alana Tinkler

one of the signal developments of the past year as policymakers in Washington, London, and other allied capitals magnified the impact of sanctions, export controls, import restrictions, and foreign investment reviews by frequently issuing joint guidance and tightly aligning their controls to make trade restrictions more challenging for Moscow, Beijing, and other targets to evade.

As roughly half the world's population prepares to head to the polls over the next twelve months—including in major elections in the United States, the European Union, and the United Kingdom—policymakers have little incentive to slow their use of economic coercive measures before facing their electorates. Very few politicians would be criticized for demonstrating strength against adversaries and competitors via enhanced sanctions or export controls. All the more so because tools like sanctions and export controls can be promulgated with little perceived risk and even more limited perceived cost to the governments imposing them. As a consequence, the heavy use of trade controls as a primary instrument of foreign policy appears poised to continue its growth regardless who occupies the White House, Downing Street, or any of the other halls of power up for grabs in 2024.

I. Global Trade Controls on Russia

- A. Blocking Sanctions
- B. Services Prohibitions
- C. Price Cap on Crude Oil and Petroleum Products
- D. Export Controls
- E. Countering Evasion
- F. Secondary Sanctions
- G. Import Prohibitions
- H. Possible Further Trade Controls on Russia

II. U.S. Trade Controls on China

- A. Export Controls
- B. Uyghur Forced Labor Prevention Act
- C. Industrial Policy
- D. Investment Restrictions
- E. Possible Further Trade Controls on China

III. U.S. Sanctions

- A. Venezuela
- B. Iran
- C. Myanmar
- D. Sudan
- E. Counter-Terrorism
- F. Other Major Sanctions Programs
- G. Crypto/Virtual Currencies
- H. OFAC Enforcement Trends and Compliance Lessons

IV. U.S. Export Controls

- A. Multilateral Coordination
- B. Commerce Department

V. Committee on Foreign Investment in the United States (CFIUS)

A. CFIUS Annual Report
B. Expanded Jurisdiction
C. State Law Investment Restrictions
D. Geographic Focus

VI. U.S. Outbound Investment Restrictions

A. Proposed Rulemaking
B. Public Comments and Unresolved Issues

VII. European Union

A. Trade Controls on China
B. Sanctions Developments
C. Export Controls Developments
D. Foreign Direct Investment Developments

VIII. United Kingdom

A. Trade Controls on China
B. Sanctions Developments
C. Export Controls Developments
D. Foreign Direct Investment Developments

I. Global Trade Controls on Russia

Following the Kremlin's full-scale invasion of Ukraine in early 2022, a coalition of leading democracies—including the United States, the European Union, the United Kingdom, Canada, Australia, and Japan—unleashed a historic barrage of trade restrictions on Russia. As the war in Ukraine stretched on into 2023, the United States and its allies shifted from rapidly introducing new and often novel trade controls to incrementally expanding existing measures such as blocking sanctions, services bans, export controls, and import bans. To further pressure Moscow, the United States authorized secondary sanctions on foreign financial institutions that, knowingly or unknowingly, facilitate significant transactions involving Russia's military-industrial base, and partnered with allied countries to crack down on sanctions and export control evasion. Such seemingly disparate measures were each calculated to deny Russia the capital and materiel needed to wage war in Ukraine. The European Union and the United Kingdom—each departing from their historic practice—increasingly imposed extraterritorial measures, including asset freezes on third-country entities that support Russia's war in Ukraine or that facilitate the contravention of relevant prohibitions.

These restrictions have generally been effective at "pouring sand into the gears" of Russia's war machine as the Kremlin has experienced shortages of key components such as semiconductors, employed elaborate transshipment schemes, and turned to suppliers of last resort like North Korea and Iran to restock its arsenal. Such trade restrictions also appear to be exacting a toll on Russia's broader economy as soaring defense spending has led to rising inflation, widening budget deficits, and forgone investment in priorities such as education and healthcare that threaten to sap Russia's long-term growth prospects. By imposing countermeasures that restrict companies' ability to depart Russia, including an "exit tax" and outright asset seizures, Moscow risks further chilling foreign investment. Meanwhile, the coalition continues to hold a handful of policy options in reserve. Depending upon events on the ground and political dynamics at home, U.S. and allied officials could in coming months escalate economic pressure on Russia by designating additional sanctions and export control evaders, further restricting exports of

sensitive components, or severing from the U.S. financial system one or more foreign banks for enabling Russia's ongoing military campaign. They could even go after various third rails in Russia—further restricting gas flows and potentially seizing Russian state assets (including central bank assets) held abroad.

A. Blocking Sanctions

Since February 2022, the United States, the European Union, and the United Kingdom, in an extraordinary burst of activity, have each added thousands of new Russia-related individuals and entities to their respective consolidated lists of sanctioned persons. While the lists do not entirely overlap, which has increased the compliance burden on multinational firms, the level of coordination among the allies has magnified the impact of sanctions by making them more challenging to evade. Underscoring the breadth of new sanctions designations, the United States on seven occasions this past year alone added 100 or more new Russia-related targets to OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List—an astonishing pace considering that around 10,000 parties had been added to the SDN List over the preceding twenty years combined. The European Union also designated more than 100 individuals and entities as part of its Russia sanctions program on three separate occasions, and the United Kingdom reached similar heights on two occasions, in 2023. This pace of change, combined with the breadth and depth of such changes, has made it increasingly difficult for the private sector to keep up.

Blocking sanctions are arguably the most potent tool in a country's sanctions arsenal, especially for countries such as the United States with an outsized role in the global financial system. Upon becoming designated an SDN (or other type of blocked person), the targeted individual or entity's property and interests in property that come within U.S. jurisdiction are blocked (i.e., frozen) and U.S. persons are, except as authorized by OFAC, generally prohibited from engaging in transactions involving the blocked person. The same applies to persons designated by the European Union or the United Kingdom. The SDN List, and its EU and UK equivalents, therefore function as the principal sanctions-related restricted party lists. Moreover, the effects of blocking sanctions often reach beyond the parties identified by name on these lists. By operation of OFAC's Fifty Percent Rule (or, in the EU and the UK, the even broader ownership *and* control tests), restrictions generally also extend to entities owned 50 percent or more in the aggregate by one or more blocked persons (or, in the EU and the UK, entities that are majority-owned *or* controlled by blocked persons), whether or not the entity itself has been explicitly identified.

During 2023, the allies repeatedly used their targeting authorities to block Russian political and business elites, as well as substantial enterprises operating in sectors such as banking, energy, and technology seen as critical to financing and sustaining the Kremlin's war effort. Notable designations included:

- Government officials, including Russian cabinet ministers and regional governors;
- Russian oligarchs such as Petr Aven, Mikhail Fridman, German Khan, and Alexey Kuzmichev—many of whom were already targeted by the European Union and the United Kingdom—plus wealthy associates of Belarus's President Alyaksandr Lukashenka;
- Financial institutions, including ***Credit Bank of Moscow*** and ***Tinkoff Bank***, as a result of which over 80 percent of Russia's banking sector by assets is now sanctioned;
- Energy firms such as ***Arctic Transshipment LLC*** and ***LLC Arctic LNG 2***, which were targeted to limit Russia's current energy revenues and future extractive capabilities;
- Military-industrial firms, including hundreds of companies operating in the technology, defense and related materiel, construction, aerospace, and

manufacturing sectors of Russia's economy, dealings with which (as discussed further below) can now place foreign financial institutions at risk of being cut off from the U.S. financial system; and

- Third-country facilitators of sanctions and export control evasion, including shipping companies and vessels alleged to have violated the price cap on Russian crude oil and petroleum products, plus dozens of parties located in major transshipment hubs such as Turkey, the United Arab Emirates, and China.

Many of the parties described above were designated pursuant to Executive Order ("E.O.") 14024, which authorizes blocking sanctions against persons determined to operate or have operated in certain sectors of the Russian Federation economy identified by the U.S. Secretary of the Treasury.

In addition to naming more than 1,000 new Russia-related individuals, entities, vessels, and aircraft to their respective sanctions lists, the United States and the European Union this past year continued to expand the potential bases upon which parties can become designated for engaging with Russia. The European Union introduced a new criteria for designation whereby persons who benefit from the forced transfer of ownership or control over Russian subsidiaries of EU companies can become subject to asset freeze measures. Meanwhile, building upon the ten sectors that had been identified in prior years, the Biden administration during 2023 authorized the imposition of blocking sanctions on parties that operate in Russia's metals and mining, architecture, engineering, construction, manufacturing, and transportation sectors—which appear to have been selected for their potential to generate hard currency or to, directly or indirectly, contribute to Russia's wartime production capabilities. Crucially, OFAC has indicated that parties operating in those sectors are *not* automatically sanctioned, but rather risk becoming sanctioned if they are determined by the Secretary of the Treasury to have engaged in targeted activities. That said, after initially treading lightly around Russian oil, gas, and metals producers to avoid roiling global markets, the Biden administration in recent months has shown a growing willingness to impose blocking sanctions on participants in Russia's extractive industries, as well as on third-country sanctions and export control evaders. These trends appear poised to continue during the year ahead.

B. Services Prohibitions

Since the opening months of the war in Ukraine, the United States, the European Union, and the United Kingdom have supplemented their use of blocking sanctions by banning the exportation to Russia of certain professional, technical, and financial services—especially including services used to bring Russian energy to market.

Executive Order 14071 prohibits the exportation from the United States, or by a U.S. person, of any category of services as may be determined by the Secretary of the Treasury, to any person located in the Russian Federation. Acting pursuant to that broad and flexible legal authority, the United States during the first year of the war barred U.S. exports to Russia of ten categories of services that, if misused, could enable sanctions evasion, bolster the Russian military, and/or contribute to Russian energy revenues. In May 2023, the United States expanded upon those earlier prohibitions by barring the exportation to Russia of architecture and engineering services in a seeming effort to prevent U.S. technical expertise from being used to enhance Russia's energy and military infrastructure.

The European Union and the United Kingdom have similarly prohibited the provision of a range of professional services to entities in Russia, subject to limited exceptions. During the past year, the European Union tweaked the range of available derogations and exceptions and expanded the scope of its professional services restrictions to include the provision of software for the management of enterprises and software for industrial design and manufacture. The United Kingdom implemented a new, strictly framed ban on the provision of legal advisory services—which temporarily froze the ability of lawyers in the

country to advise on a wide scope of even Russia-related issues. Fortunately, this situation was eased by the issuance of a general license shortly thereafter.

Those incremental adjustments aside, over the past year the allies chiefly focused on implementing and enforcing a novel form of services ban designed to cap the price of seaborne Russian crude oil and petroleum products.

C. Price Cap on Crude Oil and Petroleum Products

Effective December 5, 2022, the United States, Canada, France, Germany, Italy, Japan, and the United Kingdom, alongside the European Union and Australia (collectively, the "Price Cap Coalition"), prohibited the provision of certain services that support the maritime transport of Russian-origin crude oil from Russia to third countries, or from a third country to other third countries, unless the oil has been purchased at or below a specified price. A separate price cap with respect to Russian-origin petroleum products became effective on February 5, 2023. The types of services that are potentially restricted varies modestly among the Price Cap Coalition countries, but generally includes activities such as brokering, financing, and insurance. A detailed analysis of the price cap, and how it is being implemented by key members of the Price Cap Coalition, can be found in a previous client alert.

From a policy perspective, the price cap is intended to curtail Russia's ability to generate revenue from the sale of its energy resources, while still maintaining a stable supply of these products on the global market. The measure is also designed to avoid imposing a blanket ban on the provision of *all* services relating to the transport of Russian oil and petroleum products, which could have far-reaching and unintended consequences for global energy prices. Accordingly, the price cap functions as an exception to an otherwise broad services ban. Best-in-class maritime service providers, which are overwhelmingly based in Price Cap Coalition countries, are permitted to continue supporting the maritime transport of Russian-origin oil and petroleum products, but only if such oil or petroleum products are sold at or below a certain price.

After spending much of the prior year designing the price cap mechanism, the coalition during 2023 shifted to implementing and enforcing this new and untested policy instrument—and were quickly met with Russian efforts at circumvention. For example, tankers carrying Russian crude oil sold above the price cap have reportedly used deceptive practices such as falsifying location data and transaction documents to continue availing themselves of coalition services. Such activities prompted OFAC in April 2023 to publish an alert warning that shipments from Russia's Pacific coast, including especially the port of Kozmino where a substantial oil pipeline terminates, may present elevated risks of price cap evasion.

As the year progressed, Russia-related parties heavily invested in building a so-called "shadow fleet" that, instead of illicitly using Price Cap Coalition service providers, seeks to avoid coalition services altogether. Broadly speaking, the shadow fleet (also known as the "ghost fleet") involves an alternative ecosystem of hundreds of aging and questionably seaworthy oil tankers, backed by sub-standard insurers, that operate outside the jurisdiction of Price Cap Coalition countries. By virtue of their age, opaque ownership, and questionable financial backing, such oil tankers are at high risk of accidents and unlikely to bear the cost of damage to other vessels or the environment. As a consequence, many ports refuse calls by these vessels. Nevertheless, as these vessels offer oil above the price cap and below the market price, for some jurisdictions, the economics of this oil has proven too attractive to turn down. As a result, the shadow fleet has contributed to Russian oil being sold at an increasingly narrow discount to global prices. Over the long term, this could further undercut the price cap's efficacy. Coalition policymakers meanwhile cite the shadow fleet as evidence that the price cap is at least partially succeeding in diverting resources from the war in Ukraine. In short, said one U.S. official, "buying tankers makes it harder for the Kremlin to buy tanks."

Amid questions about the price cap's continuing effectiveness, the coalition during the final months of the year pivoted to a second phase of implementation that has so far involved imposing blocking sanctions on a small, but growing, number of maritime industry participants and issuing updated guidance to compliance-minded companies.

Notably, OFAC in October, November, and December 2023, and continuing in January 2024, added a total of 39 shipping companies, vessels, and oil traders to the SDN List for their alleged involvement in using Price Cap Coalition service providers to transport Russian-origin crude oil priced above $60 per barrel after the price cap policy became effective. Such limited designations appear to have been calibrated as a series of warning shots—reflecting the delicate balance that policymakers face in deterring market participants from facilitating the transport of high-priced Russian oil without clamping down so aggressively as to spook financial institutions, shippers, and oil traders away from lawful dealings in Russian oil, which could reduce supply and drive up global energy prices. Moreover, policymakers are being careful to balance broader geopolitical interests to avoid seeing the rest of the BRICS, for example, more aggressively support Moscow's revanchism. Even so price cap-related designations appear highly likely during the months ahead.

Concurrent with the initial round of designations described above, the Price Cap Coalition in October 2023 published an advisory describing for maritime oil industry participants, including governmental and private sector actors, suggested best practices to minimize the risk of enabling a prohibited transaction involving Russian oil. Although many of the advisory's suggestions hew closely to the U.S. Government's 2020 Global Maritime Sanctions Advisory, such as monitoring for signs that a vessel has improperly disabled its location-tracking Automatic Identification System and/or engaged in ship-to-ship transfers, the coalition also offers a number of price cap-specific recommendations. Among other measures, industry participants are encouraged to require oil tankers to carry legitimate and properly capitalized insurance; be certified as seaworthy by a reputable classification society; and furnish itemized invoices that separately list all ancillary costs (e.g., shipping, insurance, freight) so that the price at which the underlying Russian oil was sold can be readily determined.

To steer clear of a potential enforcement action, service providers from Price Cap Coalition countries that deal in seaborne Russian crude oil or petroleum products need to be able to provide certain evidence that the price cap was not breached in respect of the shipment that they are servicing. For example, the United States, the European Union, and the United Kingdom have each set forth a detailed recordkeeping and attestation process by which maritime transportation industry actors can benefit from a "safe harbor" from prosecution arising out of violations by third parties. In December 2023, the Price Cap Coalition released more stringent guidance requiring service providers based in Price Cap Coalition countries to collect attestations with greater frequency and to gather more granular pricing information. To benefit from the safe harbor, covered service providers now must receive attestations each time they lift or load Russian-origin oil or petroleum products, and must also retain, provide, or receive an itemized list of ancillary costs such as shipping, insurance, and freight, which additional information is designed to prevent transaction parties from obscuring the price at which Russian oil was sold.

In parallel, the European Union in December 2023 moved to bolster the price cap by requiring EU operators to obtain authorization from a national competent authority prior to selling or transferring ownership of an oil tanker to a Russian individual or entity, or for use in Russia. EU operators must also notify a national competent authority of each sale or transfer of a tanker to parties based in third countries (i.e., other than the European Union or Russia). These EU measures are calculated to stunt the growth of Russia's shadow fleet.

D. Export Controls

During 2023, the United States, the European Union, and the United Kingdom continued

to find ways to expand their already unprecedented range of export controls targeting Russia and Belarus. Many of these changes either build upon novel controls introduced in 2022, or seek to align each jurisdiction's existing controls with those implemented by allies and partners.

In conjunction with the first anniversary of Russia's further invasion of Ukraine, the U.S. Department of Commerce's Bureau of Industry and Security in February 2023 announced significant expansions of the Russian and Belarusian Industry Sector Sanctions, including the addition of over 500 items, identified by Harmonized Tariff Schedule ("HTS") codes, to lists of commercial, industrial, and luxury items that now require an export license for Russia or Belarus. The agency's use of HTS codes—which are widely used around the globe for classifying goods—appears to have been driven by a policy interest in expanding the reach of U.S. export controls beyond the items identified on BIS's Commerce Control List. Rather, BIS is now increasingly relying on a common tool (the HTS codes) that will allow for greater coordination and interoperability with restrictions put in place by allied and partner countries, while also enabling BIS to control exports of commercial items that, under U.S. regulations, are designated EAR99. After Iranian unmanned aerial vehicles ("UAVs") appeared on the battlefield in Ukraine, in some cases with U.S.-branded parts and components, BIS also announced new controls on commercial items that are used in the production of UAVs when destined for Iran, Russia, Crimea, or Belarus. Notably, the new UAV-related controls reach foreign-made products when such items rely upon certain U.S.-origin software or technology through the application of a new Iran-related Foreign Direct Product Rule.

From May 2023 to January 2024, BIS added over 1,300 items to the list of electronics, industrial items, manufacturing equipment, and materials that require an export license to Russia or Belarus. As a result, under U.S. law, four entire chapters of the Harmonized Tariff Schedule are now subject to an export licensing requirement when goods identified in those chapters—including nuclear items (Chapter 84); electrical machinery and equipment (Chapter 85); aircraft, spacecraft, and parts thereof (Chapter 88); and optical, photographic, precision, medical, or surgical instruments (Chapter 90)—are destined for Russia or Belarus. These and other updates brought U.S. controls on commercial items into closer harmony with controls imposed by the European Union and the United Kingdom, which have generally imposed controls based on their equivalents to the HTS codes used by the United States. BIS also updated the list of jurisdictions that have implemented substantially similar export controls targeting Russia and Belarus to include Taiwan alongside 37 previously identified countries. This list exempts these partner jurisdictions from U.S. controls on commercial items.

New measures implemented by the European Union and the United Kingdom track the trends discussed above. For instance, the European Union's twelfth Russia sanctions package imposed new export restrictions on dual-use items, advanced technology, and industrial goods worth €2.3 billion per year. The European Union also expanded the scope of existing export restrictions to include a prohibition on the sale, license, or transfer of intellectual property rights and trade secrets relating to several categories of goods or technology, and bolstered transit restrictions—a novel kind of export control which the United States has yet to impose. Over the course of 2023, the United Kingdom also broadened the range of goods subject to trade sanctions through various amendments to primary legislation.

In light of these expanded controls targeting Russia, divestiture transactions continue to raise thorny issues. Companies headquartered virtually anywhere in the world that desire to divest their Russian operations must now consider whether such divestment would result in the transfer of U.S.-controlled items to end users in Russia. Increasingly, such transfers trigger an export licensing requirement, including for dual-use and commercial items. Accordingly, in furtherance of the U.S. Government's policy of enabling companies to exit the Russian and Belarusian markets, BIS announced a case-by-case license review policy for license applications submitted by companies that are curtailing or closing all operations in Russia or Belarus and are headquartered *outside* of Country Groups D:1,

D:5, E:1, or E:2 (i.e., certain jurisdictions that present heightened national security concerns, are subject to a United Nations ("UN") or U.S. arms embargo, and/or are subject to a U.S. trade embargo). The European Union has introduced similar new grounds on which national competent authorities may authorize the sale, supply, or transfer of listed goods and technology, along with associated intellectual property, in the context of transactions that are strictly necessary for divestment from Russia or the wind-down of business activities in Russia. Parallel provisions have been implemented by the United Kingdom and fleshed out in published guidance.

In addition to these regulatory changes, BIS maintained a heavy focus on Russia-related enforcement. As discussed in more detail below, in 2023 the agency's Office of Export Enforcement had a banner year, including the launch of the Disruptive Technology Strike Force in partnership with the U.S. Department of Justice ("DOJ") to bring criminal enforcement actions against individuals and entities that circumvent export controls on Russia, China, and Iran. In some cases, criminal enforcement actions by DOJ were accompanied by the addition of Russia-related parties to the Entity List. In 2023, BIS added well over 100 new entities to the Entity List under the destination of Russia alone, as well as many other entities located around the world, including in allied and partner countries, for allegedly supplying Russia's defense sector with U.S.-origin goods, including semiconductors, electronics, and aviation equipment.

E. Countering Evasion

In addition to imposing new sanctions and export controls, the United States and its allies devoted considerable resources to shoring up existing trade restrictions on Russia by working to limit opportunities for evasion. Such efforts involved a high degree of interagency and international coordination, including the provision of substantial external guidance designed to better equip the private sector to detect, prevent, and report on Russian attempts to circumvent U.S. and allied trade controls. These multi-jurisdictional, joint guidance documents often emphasized practical sets of "red flags" to help identify evasion efforts and articulated heightened due diligence and compliance expectations by U.S. and allied regulators, especially when transactions involve certain high-priority items with potential military applications. Taken together, these joint notices, which were once rare, suggest that coalition sanctions and export controls authorities remain hyper-vigilant for potential Russia-related trade controls violations, and Russian circumvention and evasion will likely remain a top global priority for enforcement actions going forward.

1. Interagency Collaboration

Within the United States, a constellation of federal agencies sought to undercut Russian sanctions and export control evasion by issuing a series of joint guidance documents. Like the multi-jurisdictional notices discussed above, these multi-agency releases were also historically rare, often undercut by bureaucratic challenges which appear to have subsided. In 2023, these joint agency advisories included:

- **BIS, OFAC, and DOJ (March 2023)**: Three U.S. Government agencies in March 2023 issued a joint compliance note detailing common ways in which malign actors have sought to circumvent U.S. sanctions and export controls, identifying key indicators a transaction party may be seeking to evade U.S. trade controls, and highlighting recent civil and criminal enforcement actions.
- **BIS and FinCEN (May 2023)**: Building on a first-of-its-kind joint alert published the prior year by BIS and the U.S. Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"), those same two agencies in May 2023 issued a supplemental export control evasion alert that established a new Suspicious Activity Report ("SAR") key term for financial institutions to use when reporting possible attempts to evade U.S. export controls on Russia ("FIN-2022-RUSSIABIS") and describes evasion typologies and "red flags." The introduction of a dedicated key term is designed to allow U.S. authorities to, within

the enormous volume of SARs that FinCEN receives each year, quickly identify possible instances of Russia-related evasion.

- **BIS and FinCEN (November 2023)**: BIS and FinCEN in November 2023 issued a further joint notice that expands upon the two agencies' Russia-related export control guidance to target export control evasion worldwide. The November joint notice announced the creation of a second new Suspicious Activity Report key term ("FIN-2023-GLOBALEXPORT") that financial institutions can use to report transactions that potentially involve evasion of U.S. export controls globally (excluding Russia which, as noted above, has its own unique key term), and provides an expansive list of "red flag" indicators of potential evasion.
- **BIS, OFAC, DOJ, State, and Homeland Security (December 2023)**: In the broadest yet example of multi-agency guidance, in December 2023 five U.S. Government agencies issued a public advisory concerning sanctions and export control evasion in the maritime transportation industry. In that document, U.S. authorities indicate that maritime actors are expected to "know your cargo," highlight tactics employed by bad actors to facilitate the illegal transfer of cargo, and note maritime industry-specific "red flags" such as ship-to-ship transfers and unusual shipping routes.

While the U.S. agencies described above have closely collaborated since the outbreak of the war in Ukraine, the volume of joint guidance and the extent of cooperation between sister agencies this past year were unprecedented and suggest that going forward the United States is likely to further break down silos between international trade disciplines in favor of a whole-of-government approach to countering sanctions and export control evasion. Although enhanced enforcement will impose even greater risks on the private sector, the collaboration between agencies will hopefully portend a more unified approach which could make compliance more straightforward.

2. International Collaboration

Beyond collaborations within the U.S. Government, the United States and its allies and partners joined together over the past year to limit Russian sanctions and export control evasion. Notable multilateral guidance focused on Russian circumvention included:

- **REPO Task Force (March 2023)**: Established within days of the Kremlin's full-scale invasion of Ukraine, the Russian Elites, Proxies, and Oligarchs ("REPO") Task Force is an information-sharing partnership of allied finance and justice ministries designed to promote joint action on sanctions, asset freezing, asset seizure, and criminal prosecution. In March 2023, the REPO Task Force issued a global advisory that identifies Russian sanctions evasion typologies, including conducting dealings through family members and close associates, using real estate to conceal ill-gotten gains, and accessing the international financial system through enablers such as lawyers, accountants, and trust service providers.
- **Five Eyes (September 2023)**: The longstanding intelligence-sharing partnership known as the Five Eyes—comprising Australia, Canada, New Zealand, the United Kingdom, and the United States—in June 2023 committed to extend their cooperation to include coordinating on export control enforcement. In September 2023, the Five Eyes followed through on that commitment by publishing joint guidance for industry and academia identifying certain high-priority items such as integrated circuits and other electronic components, organized by Harmonized System ("HS") code, that present heightened risk of being diverted to Russia for use on the battlefield in Ukraine.
- **United States, European Union, United Kingdom, and Japan (May to October 2023)**: In parallel with efforts by the Five Eyes, the United States, the European Union, the United Kingdom, and Japan published and periodically updated a common list of high-priority items that, as of this writing, identifies by HS code 45 items deemed especially high risk for diversion due to their potential use in

Russian weapons systems. By widely disseminating a uniform list of items, coalition members sought to align controls across jurisdictions and concentrate finite compliance resources on a subset of items considered crucial to the Russian war effort.

3. Key Red Flags

The joint notices, alerts, and guidance described above each offer practical guidance to the private sector on detecting potential Russian evasion and circumvention, including identifying techniques commonly used to conceal the end user, final destination, or funding source for a transaction. Although those documents are designed for different audiences and each contain a subtly different set of recommendations, several common "red flags" for Russian sanctions and export control evasion recur across nearly all the multiagency and multilateral guidance issued in 2023 and include:

- Use of complex or opaque corporate structures to obscure ownership, source of funds, or countries involved;
- Reluctance by parties to provide requested information, including the names of transaction counterparties, beneficial ownership details, or written end-user certifications; and
- Transaction-level inconsistencies such as publicly available information regarding the counterparty (e.g., address, website, phone number, line of business) that appears at odds with an item's purported use or destination. In part, this guidance seeks to address the ever-growing challenge of transshipment and diversion in which legal exports to a third country wind up being reexported to Russia or other jurisdictions of concern.

A further recurring theme of guidance issued over the past year is the importance of private sector cooperation to the success of U.S. and allied trade controls on Russia, and heightened expectations on the part of U.S. and allied regulators concerning private sector compliance. Many of these notices reiterate the expectation that private actors adopt risk-based compliance measures, including management commitment, risk assessments, internal controls, testing and auditing, training, empowering staff to report potential violations, and seeking written compliance certifications for higher-risk exports.

F. Secondary Sanctions

As part of a broader effort to limit sanctions and export control evasion, the United States in an unprecedented escalation of pressure on Moscow authorized secondary sanctions on foreign financial institutions that, knowingly or unknowingly, facilitate significant transactions involving Russia's military-industrial base. These new restrictive measures are noteworthy not simply because they create new secondary sanctions risks for foreign banks and other financial institutions, but also because they expose these financial institutions to such risks based on the facilitation of trade in certain enumerated goods, and do so under a standard of strict liability (i.e., without requiring any culpable mental state such as knowledge). In short, these restrictions do what many had long thought to be coming—place broader export control compliance obligations on financial institutions.

Under certain U.S. sanctions programs—namely, those targeting Iran, North Korea, Russia, Syria, and Hong Kong—persons outside of U.S. jurisdiction that engage in enumerated transactions with certain targeted persons or sectors, including transactions with no ostensible U.S. nexus, risk becoming subject to U.S. secondary sanctions. Such measures target certain significant transactions involving, for example, Iranian port operators, shipping, and shipbuilding. In practice, secondary sanctions are highly discretionary in nature and principally designed to prevent non-U.S. persons from engaging in certain specified transactions that are prohibited to U.S. persons. If OFAC determines that a non-U.S. person has engaged in such transactions, the agency may impose punitive measures on the non-U.S. person which vary from the relatively

innocuous (e.g., blocking use of the U.S. Export-Import Bank) to the severe (e.g., blocking use of the U.S. financial system or blocking all property interests). Until December 2023, non-U.S. persons only potentially risked secondary sanctions exposure, under the small handful of sanctions programs that include such measures, for *knowingly* engaging in certain significant transactions.

As we discuss in a prior client alert, the Biden administration on December 22, 2023 issued Executive Order 14114 and related guidance authorizing OFAC to impose secondary sanctions on foreign financial institutions that are deemed to have:

- Conducted or facilitated a significant transaction involving any person designated an SDN for operating in Russia's technology, defense and related materiel, construction, aerospace, or manufacturing sectors, or any other sector that may subsequently be determined by the U.S. Secretary of the Treasury (such persons, "Covered Persons"); or
- Conducted or facilitated a significant transaction, or provided any service, involving Russia's military-industrial base, including the direct or indirect sale, supply, or transfer to Russia of specified items such as certain machine tools, semiconductor manufacturing equipment, electronic test equipment, propellants and their precursors, lubricants and lubricant additives, bearings, advanced optical systems, and navigation instruments (such items, "Covered Items").

Upon a determination by the Secretary of the Treasury that a foreign financial institution has engaged in one or more of the sanctionable transactions described above, OFAC can (1) impose full blocking measures on the institution or (2) prohibit the opening of, or prohibit or impose strict conditions on the maintenance of, correspondent accounts or payable-through accounts in the United States. Such measures are a potentially powerful deterrent to engaging in dealings involving Covered Persons or Covered Items as the potential consequence of such a transaction (i.e., imposition of blocking sanctions or loss of access to the U.S. financial system) is tantamount to a death sentence for a globally connected bank.

Critically, these new Russia-related secondary sanctions do not require that a foreign financial institution knowingly engage in such a transaction. This departs from the language that OFAC has historically used when crafting thresholds needed for the imposition of secondary sanctions. Provided that OFAC's traditional multi-factor test for whether a transaction is "significant" is met, the prospect of strict liability secondary sanctions risk—which is entirely new in U.S. sanctions—will undoubtedly alter the diligence and risk calculus for financial institutions that may still be dealing in legally permitted Russia-related trade.

Compounding the potential compliance challenges for foreign financial institutions, E.O. 14114 appears to create an extraterritorial U.S. export control-like regime in the guise of secondary sanctions. Financial institutions, including foreign financial institutions, are already subject to a certain degree of compliance obligations under U.S. export control laws when it comes to knowingly facilitating prohibited trade in items that are subject to U.S. export controls. However, with the issuance of E.O. 14114, these entities now risk losing access to the U.S. financial system for even inadvertently engaging in a transaction involving Covered Items—regardless whether such items are subject to a U.S. export licensing requirement—destined for Russia.

E.O. 14114 will likely cause many foreign financial institutions to reexamine their risk appetite and related controls when it comes to trade-related activity involving Russia. As a practical matter, many foreign banks, confronted with the prospect of U.S. secondary sanctions exposure and the considerable due diligence challenge of assessing whether a particular transaction might implicate Russia's military-industrial base, may end up erring on the side of overcompliance by declining to engage in otherwise lawful dealings involving Russia.

G. Import Prohibitions

Consistent with a whole-of-government approach to limiting Russian revenue, the United States, the European Union, and the United Kingdom expanded prohibitions on the importation into their respective territories of certain Russian-origin goods—principally consisting of items closely associated with Russia or that otherwise have the potential to generate hard currency for the Kremlin.

During the initial year of the war in Ukraine, the Biden administration used this particular policy tool to bar imports into the United States of certain energy products of Russian Federation origin, namely crude oil, petroleum, petroleum fuels, oils, and products of their distillation, liquified natural gas, coal, and coal products; followed by fish, seafood, alcoholic beverages, non-industrial diamonds; and eventually gold. As with other Russia-related sanctions authorities, the Secretary of the Treasury has broad discretion under Executive Order 14068 to, at some later date, extend the U.S. import ban to additional Russian-origin goods.

The United States initially excluded from its import bans Russian-origin goods that have been incorporated or substantially transformed (i.e., fundamentally changed in form, appearance, nature, or character) into another product in a third country. However, in December 2023, in tandem with the new Russia-related secondary sanctions described above, President Biden amended Executive Order 14068 to authorize the Secretary of the Treasury to prohibit the importation into the United States of certain products that have been mined, extracted, produced, or manufactured wholly or in part in the Russian Federation, or harvested in waters under the jurisdiction of the Russian Federation or by Russia-flagged vessels, *regardless* whether such specified products have been incorporated or substantially transformed into other products outside of Russia. Acting pursuant to this authority, OFAC issued a determination barring the importation into the United States of foreign-made goods that contain any amount of Russian-origin salmon, cod, pollock, or crab, and indicated that a similar prohibition on importing certain Russian diamonds processed in third countries is expected to follow soon. Similarly, the European Union and the United Kingdom adopted an import ban on iron and steel products processed in a third country using Russian iron or steel products. Such enhanced import prohibitions on a narrow subset of products (i.e., certain fish, certain diamonds, iron and steel products) will likely present considerable practical challenges—similar to the Uyghur Forced Labor Prevention Act with respect to goods linked to China's Xinjiang Uyghur Autonomous Region—for importers who may now be required to demonstrate that their supply chains do not, directly or indirectly, trace back to Russia.

The European Union and the United Kingdom during 2023 also expanded the range of Russian goods subject to more traditional import prohibitions. Notable additions include diamonds and various metals, delivering a further blow to the Kremlin's ability to finance its war in Ukraine and other destabilizing activities globally.

H. Possible Further Trade Controls on Russia

Leading democracies in 2023 continued to expand the dizzying array of trade restrictions imposed on Russia. While the coalition has not yet exhausted its policy toolkit, barring dramatic developments on the ground, the coming year appears likely to be defined by a further tightening of restrictions on Moscow.

Policymakers in Washington, London, and other allied capitals appear poised to continue aggressively blacklisting third-country sanctions and export controls evaders. To stanch the flow of sensitive components to the Russian military, the coalition may further expand its common list of high-priority items to subject additional goods to heightened scrutiny. The United States could also leverage its new Executive Order 14114 to secondarily sanction one or more foreign financial institutions—severing their access to mainstream finance—as a warning to other banks considering engaging with Russia's military-industrial base.

More severe measures—such as blocking sanctions on the Government of the Russian Federation or conceivably a complete embargo on Russia like the U.S. measures that presently apply to Cuba, Iran, North Korea, Syria, and certain Russian-occupied regions of Ukraine—also remain available. However, in light of wavering political support for Kiev in some allied capitals, a seeming stalemate on the battlefield, and the imperative of maintaining stable energy prices, such restrictions appear unlikely to be imposed in the near term absent a complete breakdown in relations with Moscow.

II. U.S. Trade Controls on China

Despite the continuing challenge posed by Russia, the year in trade was largely defined by the deepening economic, technological, and security rivalry between the United States and China. Following a year marked by high tensions over Taiwan and a near-total breakdown in communications, relations between Washington and Beijing gradually stabilized in 2023, culminating in a long-awaited summit at which President Biden and China's President Xi Jinping pledged to responsibly manage competition between the two superpowers.

That brief moment notwithstanding, U.S. officials from across the political spectrum continue to view China—with its rapidly advancing military and technological capabilities, state-led economy, and troubling human rights record—as the "pacing challenge" for U.S. national security. To meet that perceived threat, the United States during 2023 again pushed the limits of economic statecraft by expanding export controls on semiconductors and supercomputers, vigorously enforcing import prohibitions on goods linked to forced labor, heavily subsidizing domestic manufacturing, scrutinizing inbound Chinese investments, and for the first time ever putting into place a system that will restrict outbound investments into certain sensitive technologies. With U.S. elections in November 2024 and bipartisan consensus on the perceived strategic threat that China poses to the United States and its allies, the pace of new trade controls on China seems unlikely to slow any time soon. One of the only questions is whether Congress or the Executive will take the lead.

A. Export Controls

Despite a mild thawing in U.S.-China relations following the November 2023 summit between Presidents Biden and Xi, controlling the manufacture and supply of certain advanced technologies remained a core feature of U.S. trade policy toward Beijing. During 2023, the United States aggressively employed a range of export control measures to slow China's technological development, including further restricting exports of certain advanced semiconductors and supercomputers, adding over 100 Chinese organizations to BIS's Entity List, and using the threat of further additions to the Entity List to incentivize Chinese firms (and the Chinese government) to permit timely end-use checks on authorized exports.

1. Expanded Controls on Semiconductors and Supercomputers

On October 17, 2023, the U.S. Department of Commerce's Bureau of Industry and Security announced two new interim final rules updating and expanding certain export controls targeting advanced computing integrated circuits ("Advanced ICs"), computer commodities that contain such Advanced ICs, and certain semiconductor manufacturing equipment ("SME"). These two interim final rules build upon the groundbreaking and extensive unilateral controls implemented by the United States in October 2022. Detailed descriptions of the original and expanded controls can be found in our client alerts published in October 2022, February 2023, and October 2023.

The October 2023 interim final rules are designed to strengthen, expand, and reinforce the original October 2022 rules, which curtailed China's ability to purchase and manufacture Advanced ICs for use in advanced weapon systems and other military applications of artificial intelligence ("AI"), products that enable mass surveillance, and other technologies

used in the abuse of human rights. Broadly speaking, the new interim final rules impose controls on additional types of SME, refine the restrictions on U.S. persons to ensure U.S. companies cannot provide support to advanced SME in China, expand license requirements for the export of SME to apply to additional countries, adjust the licensing requirement criteria for Advanced ICs, and impose new measures to address risks of circumvention of the controls by expanding them to additional destinations.

Perhaps the most significant development in the new interim final rules is the expansion of certain controls to destinations beyond China (including the Hong Kong special administrative region) and the Macau special administrative region. Namely, the interim final rule on advanced computing items and supercomputer and semiconductor end uses expands the previous controls to 21 other destinations for which the United States maintains an arms embargo (i.e., so-called Country Group D:5 countries) and revises a previously imposed foreign direct product rule targeting non-U.S.-origin products used in advanced computing and supercomputers to apply to these same Country Group D:5 destinations. Similarly, the interim final rule on SME items expands the relevant controls to an additional 44 destinations (i.e., all destinations specified in Country Groups D:1, D:4, and D:5, excluding Cyprus and Israel). The expanded destination scope of these rules is intended to account for the possibility that counterparties located in these jurisdictions might try to obtain these highly controlled items for end users in other destinations and to apply the prohibitions to the longer list of countries that the United Nations and the United States have identified as posing heightened risks.

Apart from expanding the territorial application of the previous rules, the two interim final rules similarly refine the item-specific Export Control Classification Numbers ("ECCNs") subject to the heightened controls. BIS abandoned the previous ECCN 3B090 introduced in the October 2022 version of the regulations and instead determined that identifying specific SME for control in ECCNs 3B001 and 3B002 represents a more manageable arrangement. BIS also refined the Advanced ICs captured under existing controls by adding a new "performance density" parameter to prevent users from purchasing and combining a large number of smaller datacenter AI chips to equal the computing power of more powerful chips already restricted under the previous controls. And BIS added new ".z" paragraphs to ECCNs 3A001, 4A003, 4A004, 4A005, 5A002, 5A004, 5A992, 5D002, and 5D992 to enable exporters to more easily identify products that incorporate Advanced ICs and items used for supercomputers and semiconductor manufacturing that meet or exceed the newly refined performance parameters.

Some of the most far-reaching restrictions contained in the October 2022 controls are the restrictions BIS placed on U.S. person support for the development and production of Advanced ICs and SME in specified jurisdictions, even when such activities did not involve items subject to the U.S. Export Administration Regulations ("EAR"). In the interim final rules, BIS both clarified and expanded these prohibitions, while codifying some of the guidance previously provided in the agency's October 2022 Frequently Asked Questions. Specifically, BIS broadened these controls to extend to U.S. person support for development or production of Advanced ICs and SME at any facility of an entity headquartered in, or whose ultimate parent company is headquartered in, either Macau or a country subject to a U.S. arms embargo where the production of Advanced ICs occurs (i.e., Country Group D:5 countries). At the same time, BIS clarified that its facility-focused support prohibition is intended to include facilities engaged in all phases of production, including where important late-stage product engineering or early-stage manufacturing steps, among others, may occur. However, BIS narrowed its facility-based prohibition in one important respect, by limiting the scope of the restrictions to exclude "back-end" production steps such as assembly, testing, or packaging steps that do not alter the technology level of an Advanced IC. Importantly, BIS also added an exclusion to the new restrictions for U.S. persons employed or working on behalf of a company headquartered in the United States or a closely allied country (i.e., destinations specified in Country Group A:5 or A:6) and not majority owned by an entity that is headquartered in Macau or a destination specified in Country Group D:5.

In conjunction with BIS's expanded destination and item-based licensing requirements, BIS issued two new temporary general licenses, valid through the end of 2025, that authorize companies headquartered in the United States and closely allied countries to continue shipping less sensitive items to certain facilities in Country Group D:1, D:4, and D:5 locations. These authorizations appear to be driven by a U.S. policy interest in enabling such companies to continue using facilities located in a restricted destination to perform more limited manufacturing tasks such as assembly, inspection, testing, quality assurance, and distribution in order to allow additional time for Advanced IC and SME producers located in the United States and closely allied countries to identify alternative supply chains outside of these more-restricted destinations.

BIS also created a new license exception—Notified Advanced Computing ("NAC")—that authorizes exports of certain less-powerful Advanced ICs and associated items to Country Group D:1, D:4, and D:5 destinations. For items ultimately intended for Macau or a destination specified in Country Group D:5, advanced notice and approval from BIS is required, a process that enables BIS to monitor and track which end users are seeking these Advanced ICs and for what purpose. In particular, at least 25 days prior to any export or reexport to Macau or a destination specified in Country Group D:5, an application must be submitted via BIS's Simplified Network Application Process Redesign ("SNAP-R") system. BIS will review any such applications and render a decision within the allotted 25 days as to whether the use of License Exception NAC is permitted. The export must also be made pursuant to a written purchase order, unless the export is for commercial samples, and cannot involve any prohibited end users or end uses (including "military end users" or "military end uses," as defined in the EAR). Exporters are also required to report their use of License Exception NAC in their export clearance filings (i.e., electronic export information, or EEI, filings).

Although the two new interim final rules provide much-needed guidance, they also make it evident that BIS has high expectations for the private sector to be at the forefront of handling complex due diligence. Given the need to review multiple information sources, even including a counterparty's aspirational development or production of technology, this type of screening is especially difficult to automate, and companies with relevant products will need to expend more compliance resources to fully address BIS's heightened diligence expectations.

In December 2023, BIS released limited guidance concerning the application of these new interim final rules, including the process for calculating "performance density" used to determine the threshold for Advanced ICs, the information needed for the use of License Exception NAC, the scope of the new temporary general licenses, and clarifications on the new exclusions from prohibited U.S. person activities. However, based upon the number and variety of requests for public comment included in the two interim final rules, further refinements and possible future expansions of these controls appear likely. BIS specifically requested public comments on a number of issues implicated by the interim final rules, including the impact of potential controls on datacenter infrastructure-as-a-service offerings for AI training and suggestions for further refining technical parameters to distinguish Advanced ICs and computers commonly used for small- or medium-scale training of AI foundational models from those used for large AI foundational models with different capabilities of concern.

Apart from the imposition of new unilateral controls, the Biden administration continues to engage in extensive diplomatic efforts to encourage closely allied countries to adopt similar controls on chip-making equipment. In advance of any nascent multilateral regimes, the new export controls imposed by the United States reflect an effort to minimize some of the known collateral impacts that current unilateral controls could have on international trade flows, especially on the Advanced IC and SME supply chains of U.S. and allied country companies, and to encourage a collective "friend-shoring" of U.S. and allied country supply chains for critical technologies. To what extent such efforts will hinder or help the development of additional multilateral controls remains to be seen, though recent actions by the Japanese and Dutch governments to implement limited

though still meaningful controls on Advanced ICs and SME supply chains indicate some initial success in the United States' efforts to expand the new controls across multiple jurisdictions.

2. China-Related Entity List and Military End-User List Designations and Removals

In addition to novel measures such as stringent controls on semiconductors and supercomputers, the Biden administration over the last several years has used traditional export controls such as the Entity List to target China-based organizations. As noted in our 2022 Year-End Sanctions and Export Controls Update, the expanding size, scope, and profile of the Entity List now rivals OFAC's SDN List as a tool of first resort when U.S. policymakers seek to exert strategic pressure, especially against significant economic actors in major economies. 2023 saw a solidification of this trend. The United States made extensive use of the Entity List throughout the past year, designating over 150 Chinese entities—more than double the number of Chinese entities added to the same list in 2022.

Entities can be designated to the Entity List upon a determination by the interagency 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. Much like being added to the SDN List, the level of evidence needed to be included on the Entity List is minimal and far less than the "beyond a reasonable doubt" standard that U.S. courts use when assessing guilt or innocence. Despite this, the impact of being included on the Entity List can be catastrophic. Through Entity List designations, BIS prohibits the export of specified U.S.-origin items to designated entities without BIS licensing. With respect to potential licensing for Entity List exports, 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 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. (This is one of the key ways in which the Entity List differs from the SDN List.)

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. In many cases over the past year, BIS turned to conventional reasons for designating Chinese entities such as their providing support for China's military modernization efforts, attempting to divert or reexport goods to restricted parties, or enabling cybersecurity activities deemed threatening to U.S. national security. Other designations, however, relied on more specific justifications, often in response to current events, such as the designation of six Chinese entities in February 2023 for supporting the People's Liberation Army's "aerospace programs including airships and balloons and related materials and components" following public outcry over Chinese high-altitude balloons flying over North American airspace. More in line with designations from the past several years, the ERC in March 2023 added several entities to the Entity List for their alleged involvement in human rights violations such as high-tech surveillance of minority groups in China's Xinjiang Uyghur Autonomous Region. Other Chinese entities were designated in June 2023 for providing "cloud-based supercomputing capabilities" in support of hypersonics research conducted by China's military, while an additional 13 entities were designated in October 2023 for their involvement with the development of Advanced ICs.

Notably, during 2023 no new Chinese entities were added to BIS's non-exhaustive Military End-User ("MEU") List, which was developed to help exporters determine which organizations in Belarus, Burma, Cambodia, China, Russia, or Venezuela are considered

"military end users" for which an export license may be required. However, one previously designated entity, China-based ***Zhejiang Perfect New Material Co., Ltd***, was removed from the MEU List in September 2023 following a request for removal submitted to BIS—suggesting that, although the process can be long and cumbersome for the targeted entity, BIS is still actively considering petitions for removal, even when such entities are located in sensitive jurisdictions.

3. China-Related Unverified List Designations and Removals

As in previous years, BIS made use of the Unverified List throughout the year to incentivize named entities to comply with robust end-use checks. A foreign person may be added to the Unverified List when BIS (or U.S. Government officials acting on BIS's behalf) cannot verify that foreign person's *bona fides* (i.e., legitimacy and reliability relating to the end use and end user of items subject to the EAR) in the context of a transaction involving items subject to the EAR. This situation may occur when BIS cannot satisfactorily complete an end-use check, such as a pre-license check or a post-shipment verification, for reasons outside of the U.S. Government's control. Any exports, reexports, or in-country transfers to parties named on the Unverified List require the use of an Unverified List statement, and Unverified List parties are not eligible for license exceptions under the EAR that would otherwise be available to those parties but-for their designation to the list.

Notably, BIS in October 2022 implemented a new two-step process whereby companies that do not complete requested end-use checks within 60 days will be added to the Unverified List. If companies are added to the Unverified List due to the host country's interference, after a subsequent 60 days of the end-use check not being completed, such companies will be moved from the Unverified List to the more restrictive Entity List. That process is designed to further incentivize targeted entities—and, at least in the case of China, their home governments—to permit BIS end-use checks to proceed in a timely manner as cooperative entities can be rewarded with removal from the Unverified List and uncooperative entities risk becoming subject to even more stringent controls.

This seemingly subtle policy change appeared to pay dividends during 2023 as a total of 32 entities from China were removed from the Unverified List in August and December 2023, and continuing in January 2024, after BIS was able to verify their *bona fides* through an end-use check—suggesting a willingness on the part of Chinese authorities to change their behavior to retain access to U.S.-origin items.

B. Uyghur Forced Labor Prevention Act

2023 marked the first full year of enforcement of the Uyghur Forced Labor Prevention Act ("UFLPA"). As we describe in a prior client alert, that groundbreaking law, which took effect in June 2022, establishes a rebuttable presumption that all goods mined, produced, or manufactured even partially within China's Xinjiang Uyghur Autonomous Region ("Xinjiang"), or by entities identified on the UFLPA Entity List, are the product of forced labor and are therefore barred from entry into the United States. After a year of active enforcement by U.S. Customs and Border Protection ("CBP"), recent calls from Congress to further strengthen and expand enforcement signal a continued focus on the UFLPA in the year ahead.

Despite criticisms that progress has been too slow, in 2023 the U.S. Government made notable additions both to CBP's list of high-risk commodities for priority UFLPA enforcement, as well as to the UFLPA Entity List maintained by the U.S. Department of Homeland Security ("DHS"). CBP's release of a document attached to UFLPA detention notices confirmed an expansion of scrutiny from products previously identified as high-risk (i.e., tomatoes, cotton, polysilicon, polyvinyl chloride, and aluminum) to now include batteries, tires, and steel products. These newly added targets, which appear to have stemmed from private sector research published in late 2022 on possible links to Xinjiang in automotive supply chains, highlight continuing close coordination between DHS and the

non-governmental and academic communities in identifying risks and specific parties of concern. Throughout 2023, the interagency Forced Labor Enforcement Task Force, led by DHS, also added 10 entities (and some of their subsidiaries) to the UFLPA Entity List. One of these entities, ***Ninestar Corporation***, has since challenged its designation before the U.S. Court of International Trade, citing a lack of information provided by DHS regarding the reasons for its listing. The outcome of that case could have broader implications for the type and extent of information that agencies are required to provide to individuals and entities that are added to U.S. Government restricted party lists.

Notably, CBP sought to increase transparency regarding UFLPA enforcement, and published additional guidance to importers concerning the law's broad standards and high bar for challenging potential detentions at U.S. ports. The launch of the UFLPA Statistics Dashboard on CBP's website in March 2023 has provided key insights into the number, value, and type of shipments detained under the UFLPA to date. As of November 2023, over 6,000 shipments had been detained under the UFLPA, valued at more than $2.2 billion. Despite the UFLPA's focus on and close association with China, the majority of goods detained to date have somewhat surprisingly originated from countries *other* than China, including Malaysia, Vietnam, and Thailand. This serves as an important reminder both of transshipment risk given today's global supply chains and the critical role of Chinese materials in supply chains of companies throughout the world and especially in Southeast Asia.

CBP statistics further reveal that slightly more than half of all shipments detained to date under the UFLPA have ultimately been released into the United States. In light of the lack of reporting to Congress of any granted "exceptions" to the UFLPA's rebuttable presumption, as required by the statute, these releases appear to all be the result of successful "applicability reviews." CBP published guidance in February 2023 on the applicability review process, in which importers submit evidence that a given shipment is outside of the scope of the UFLPA altogether, and thus the rebuttable presumption does not apply (i.e., the goods are not mined, produced, or manufactured wholly or in part in Xinjiang or by an entity on the UFLPA Entity List). That guidance, which indicates importers must be able to submit evidence tracing their supply chains back to the raw materials, highlights the need for robust supply chain due diligence programs and the development of novel recordkeeping and contracting tools that enable buyers of goods to extend their supply chain tracing well beyond the first tier of suppliers. Although the UFLPA has its roots in Great Depression-era legislation that first restricted the importation into the United States of goods linked to forced labor, the UFLPA remains a relatively new human rights policy tool that appears ripe for further guidance and vigorous enforcement during the year ahead.

C. Industrial Policy

In a sea change from longstanding U.S. aversion to state industrial policy, the United States continued to embrace a protectionist-leaning "modern industrial and innovation strategy" to counteract China's influence on the world stage. After the U.S. Congress adopted two massive legislative packages—the CHIPS and Science Act of 2022 (the "CHIPS Act") and the Inflation Reduction Act of 2022 (the "IRA")—that direct billions of dollars toward boosting domestic manufacturing, in 2023 the Biden administration began implementing these laws by issuing multiple sets of regulations defining which parties are (and are not) potentially eligible to receive U.S. subsidies, in each case with an eye toward preventing taxpayer dollars from flowing to China.

The CHIPS Act provides over $50 billion in incentives for semiconductor manufacturers to invest in production capacity in the United States. Notably, those incentives can be clawed back if manufacturers violate so-called guardrails, mandated by Congress, barring certain investments in "countries of concern," namely China, Russia, Iran, and North Korea. In September 2023, the U.S. Department of Commerce issued a final rule implementing the CHIPS Act national security guardrails. Among other things, the rule bars recipients of CHIPS Act funding, for 10 years from the date of award, from expanding

production facilities in countries of concern by 10 percent or more for legacy chips, and by 5 percent or more for chips that are advanced or critical to U.S. national security. The rule also defines the categories of joint research and technology licensing that are prohibited under the CHIPS Act to include most activities involving entities owned or controlled by a country of concern, as well as entities identified on BIS's Entity List and OFAC's Non-SDN Chinese Military-Industrial Complex Companies ("NS-CMIC") List. From a policy perspective, the CHIPS Act guardrails are designed to prevent taxpayer-funded incentives from accruing to the benefit of China's semiconductor industry and, over time, shift the geography of semiconductor manufacturing activities away from China and toward the United States and other friendly jurisdictions.

In a parallel effort to relocate electric-vehicle ("EV") supply chains from China to the United States, the Inflation Reduction Act includes billions of dollars in subsidies for EVs assembled in North America—a move that has rankled close U.S. allies in Europe who have criticized the measure as protectionist and discriminatory against European goods. Among other limitations, the IRA stipulates that, to be eligible for an up to $7,500 tax credit, an EV must undergo final assembly in North America, a certain percentage of the critical minerals in the vehicle's battery must be extracted or processed in the United States or in a country with which the United States has a free trade agreement, and the vehicle's battery cannot contain any components manufactured in certain countries of concern such as China. To assuage allied concerns regarding the IRA, the United States in March 2023 entered into a critical minerals agreement with Japan, and is presently negotiating similar agreements with the European Union and the United Kingdom, which could enable companies based in those jurisdictions to benefit from U.S. electric-vehicle subsidies. Meanwhile, the U.S. Department of the Treasury in December 2023 issued a notice of proposed rulemaking further defining which EVs are potentially ineligible for U.S. subsidies by virtue of their ties to China. These developments, taken together, suggest a willingness on the part of the Biden administration to implement and interpret the IRA in a manner that simultaneously advantages core U.S. allies and withholds benefits from Beijing.

D. Investment Restrictions

In conjunction with export controls, the Biden administration, acting through the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), continued to closely scrutinize acquisitions of, and investments in, U.S. businesses by Chinese investors. As discussed more fully in Section V.A, below, CFIUS appears to be especially focused on identifying non-notified transactions involving Chinese acquirors (i.e., transactions that have already been completed and which were not brought to CFIUS's attention), including through use of the Committee's increased monitoring and enforcement capabilities.

During calendar year 2022, the most recent period for which data is available, Chinese investors once again eschewed the CFIUS short-form declaration process, filing only 5 declarations and 36 notices. Those figures are generally consistent with the period from 2020 to 2022. This apparent preference of Chinese investors to forgo the short-form declaration in favor of the *prima facie* lengthier notice process may indicate a calculus that, amid U.S.-China geopolitical tensions, the likelihood of the Committee clearing a transaction involving a Chinese investor through the scaled-down declaration process is quite low.

In addition to the Committee's purview over inbound investments, the Biden administration in August 2023 issued a long-awaited Executive Order and Advance Notice of Proposed Rulemaking ("ANPRM") outlining proposed restrictions on outbound investment by U.S. persons in certain mainland China, Hong Kong, and Macau entities. As discussed in Section VI, below, while there remains significant uncertainty surrounding the timing and contours of an eventual final rule, the Biden administration proposal in its current form would significantly restrict U.S. investments in certain sectors of China's economy deemed critical to U.S. national security, including artificial intelligence, semiconductor manufacturing, and quantum information technologies. Such restrictions

are highly novel and a significant departure from historical practice.

E. Possible Further Trade Controls on China

The Executive branch was not alone in pushing for stringent new trade controls on China. The U.S. Congress throughout 2023 continued to churn out legislation and policy proposals to govern the U.S.-China economic relationship—some of which enjoy strong bipartisan support. At the start of the year, the U.S. House of Representatives created the Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (the "Select Committee") to "investigate and submit policy recommendations on the status of the Chinese Communist Party's economic, technological, and security progress and its competition with the United States." The Select Committee's top Republican and Democratic members have tackled issues relating to China in a notably bipartisan manner compared to the rest of the House, including in December 2023 issuing a report with almost 150 policy recommendations to "fundamentally reset the United States' economic and technological competition with the People's Republic of China." The committee's recommendations include, among others:

- **Preventing reliance on China** for advanced technology and reducing China's access to the U.S. market by authorizing the President to ban certain Chinese-produced technology products; banning Chinese-owned social media; and funding "rip-and-replace" efforts to remove products from Chinese-owned telecommunications vendors from U.S. networks;
- **Restricting U.S. outbound investment** in more sectors than are presently covered by President Biden's August 2023 Executive Order and limiting market access for companies from foreign adversary countries by requiring them to make human rights certifications;
- **Strengthening export controls** by providing BIS increased resources and extending export licensing requirements to entities that are majority owned by one or more parties identified on BIS's Entity List—similar to OFAC's Fifty Percent Rule ; and
- **Empowering CFIUS** to review greenfield investments and joint ventures involving foreign adversary entities, streamlining the Committee's review of transactions from allied countries, and allowing the Committee to re-open mitigated transactions.

Although it is challenging for a closely divided and highly partisan Congress to negotiate and pass legislation—and there is little time left before members' attention turns to the November 2024 election—the Select Committee's bipartisan imprimatur could give these recommendations traction in the Republican-led House, but probably not in the Democratically controlled Senate. Even if not enacted this year, the Select Committee's recommendations offer hints as to the future direction of U.S. policy toward Beijing, especially if the Senate flips to Republican control after the next election. Accordingly, before further engaging with China, multinational enterprises may wish to consider the potential impact of these proposals on their business should Congress or the Executive branch decide to act on them in the coming months.

III. U.S. Sanctions

Although Russia and China dominated U.S. trade policy for much of the past year, OFAC remained extraordinarily active on other fronts—including modulating U.S. sanctions on Venezuela, Iran, Myanmar, and Sudan; leveraging U.S. counter-terrorism sanctions authorities in response to the Hamas attack on Israel in October and follow-on violence perpetrated by various Iranian proxies; heavily focusing on the virtual currency sector; and bringing record-setting enforcement actions.

A. Venezuela

Following the signing of an electoral roadmap between Venezuela's opposition and the regime of President Nicolás Maduro, the Biden administration in October 2023 announced a significant relaxation of U.S. sanctions on Venezuela. That easing of restrictions on Caracas, however, did not last long as the United States soon reversed course and partially revoked sanctions relief in January 2024 following democratic backsliding by Maduro.

As we describe in a prior client alert, the broad package of measures unveiled in October 2023—which eased restrictions on Venezuela's oil and gas sector, gold sector, and secondary trading in certain Government of Venezuela securities—marked a seismic shift from the "maximum pressure" campaign that since 2019 has prohibited virtually all U.S. nexus dealings involving key sectors of Venezuela's energy-driven economy. From a policy perspective, such incremental, and in some cases time-limited, sanctions relief was calculated to incentivize the Maduro regime to take concrete steps toward the restoration of Venezuelan democracy with an eye toward holding a free and fair presidential election in late 2024.

Among the measures announced in October 2023, the most impactful was Venezuela General License 44 which authorizes U.S. persons, until April 18, 2024, to engage in all transactions related to oil or gas sector operations in Venezuela, including transactions involving state-owned oil giant ***Petróleos de Venezuela, S.A.*** ("PdVSA"), subject to certain conditions. Crucially, that general license sets forth a non-exhaustive list of authorized activities that includes: (1) the production, lifting, sale, and exportation of oil or gas from Venezuela, and the provision of related goods and services; (2) payment of invoices for goods or services related to oil or gas sector operations in Venezuela; (3) new investment in oil or gas sector operations in Venezuela; and (4) delivery of oil and gas from Venezuela to creditors of the Government of Venezuela, including creditors of PdVSA entities, for the purpose of debt repayment.

In addition to easing sanctions on Venezuelan oil and gas, the Biden administration further broadened the Maduro regime's access to potential sources of hard currency by easing sanctions on Venezuela's gold sector. In particular, OFAC issued—and, again, later revoked—a general license authorizing most U.S. nexus transactions involving Venezuela's state-owned gold mining company, ***CVG Compania General de Mineria de Venezuela CA*** ("Minerven"), and its majority-owned entities. In a key development for investors and financial institutions, OFAC also amended a pair of general licenses to authorize U.S. persons to both sell and purchase certain specified Venezuelan sovereign bonds and specified PdVSA debt and equity, thereby permitting secondary trading in previously restricted Government of Venezuela securities.

The easing of U.S. sanctions on Venezuela was noteworthy both for its breadth and for the fact that much of the relief extended to Caracas rested on a promise by the Maduro regime to take further steps toward the restoration of Venezuelan democracy. When the regime failed to uphold its end of the bargain, including by refusing to lift a ban on a leading presidential candidate holding public office, the U.S. Government quickly revoked the general license that had authorized dealings involving the gold mining company Minerven—and indicated that, absent a change in behavior by the Maduro regime, the more economically consequential general license authorizing U.S. nexus dealings involving the country's oil or gas sector could soon meet a similar fate. As of this writing, the U.S. sanctions relief extended to Venezuela just months ago appears highly tenuous and could be revoked in its entirety in coming months—potentially causing whiplash for investors that had begun to explore collecting on old debts, and launching new energy ventures, involving Venezuela.

B. Iran

Relations between the United States and Iran took a sharp downward turn during 2023. After starting the year engaged in indirect talks over a possible return to the Joint Comprehensive Plan of Action ("JCPOA")—the 2015 Iran nuclear agreement that the

Trump administration renounced and exited in 2018—tensions between Washington and Tehran spiked following the October 2023 attack by the Iranian-supported Hamas terrorist group that claimed 1,200 civilian lives and spurred an Israeli ground invasion of the Gaza Strip. As a Middle East-wide network of Iran-backed militias dubbed the "axis of resistance," including Hamas, Hezbollah, and the Houthis, continued to mount attacks across the region—including at least one lethal assault on U.S. troops—debate quickly turned to whether the United States and Iran might come to blows. As these developments unfolded, the Biden administration announced new sanctions designations targeting Iran's UAV and ballistic missile program, petroleum and petrochemicals trade, hostage taking, and domestic repression; revoked Iranian access to funds that had been set aside for humanitarian trade; and prepared to levy further sanctions following a wave of deadly attacks by Iranian proxies.

Throughout 2023, OFAC continued to aggressively use its targeting authorities to add individuals and entities complicit in Iran's destabilizing activities to the SDN List. Frequent targets of Iran-related sanctions designations included parties allegedly involved in:

- The development, and exportation to Russia, of Iranian unmanned aerial vehicles, as well as support for Iranian ballistic missile procurement, in connection with which the U.S. Government published multiple rounds of guidance on the sanctions and export controls risks of engaging with Iran's UAV and ballistic missile programs;
- The Iranian petroleum and petrochemicals trade, including buyers and shippers based in the United Arab Emirates and China;
- The wrongful detention of U.S. nationals, including intelligence officials and Iran's former president Mahmoud Ahmadinejad; and
- The repression of dissent, including Iranian military, intelligence, and law enforcement entities and officials implicated in suppressing protests and restricting internet access.

Although the United States continued to modestly increase sanctions pressure on Iran even as the two sides negotiated over the JCPOA, including completing a September 2023 prisoner swap, relations between Washington and Tehran deteriorated following Hamas's attack on Israel. The Biden administration quickly suspended a humanitarian trade channel that would have granted Iran limited access to $6 billion held in a restricted account in Qatar. OFAC also stepped up the pace of new sanctions designations, with a particular emphasis on targeting individuals and entities associated with Iran-backed militant groups. As the Biden administration began to militarily respond to the January 2024 attack by an Iran-aligned group that left three U.S. soldiers dead, and continued leading multinational efforts against the Houthis' attacks on Red Sea shipping, the security situation in the Middle East remains highly fluid. In coming weeks and months, the United States appears highly likely to further accelerate the pace of Iran-related designations and could, in an effort to constrict Tehran's sources of funding and support, begin imposing secondary sanctions on non-U.S. parties that knowingly engage in significant transactions involving Iran.

C. Myanmar

Since seizing power in a February 2021 coup, the military junta in Myanmar (also called "Burma") has wreaked havoc on the country's civilian population through a brutal campaign of repression, including airstrikes. As the humanitarian situation continued to deteriorate, the United States in 2023 moved to restrict the flow of materiel and funding to the Myanmar military (known as the "Tatmadaw"), including by targeting dealings involving jet fuel and imposing limited sanctions on Myanmar's state-owned energy company.

Over the past several years, U.S. sanctions on Myanmar have increasingly focused on restricting transactions that could enable the Tatmadaw's human rights abuses.

Continuing this trend, OFAC in March 2023 added to the SDN List numerous individuals and entities involved in the "importation, storage, and distribution of jet fuel to Burma's military" and concurrently published guidance emphasizing that providing jet fuel to the Tatmadaw could be sanctionable under one or more of the provisions of Executive Order 14014. These efforts culminated in August 2023 with OFAC's issuance of a determination authorizing blocking sanctions on persons determined to operate in the jet fuel sector of the Burmese economy, coupled with the designation of two individuals and three entities for their alleged involvement in procuring and distributing jet fuel to Myanmar's military regime. OFAC also continued to target the junta itself by imposing blocking sanctions on Myanmar's Ministry of Defense, as well as on various military and regime officials.

In addition to targeting jet fuel, OFAC sought to limit the junta's key sources of revenue. Consistent with sanctions in prior years targeting state-owned enterprises, a round of Burma sanctions in January 2023 included the designation of two state-owned mining companies. In June 2023, OFAC designated two state-owned financial institutions, ***Myanma Foreign Trade Bank*** and ***Myanma Investment and Commercial Bank***, to deprive the regime of access to foreign exchange. In January 2024, in connection with the third anniversary of the military's seizure of power, OFAC also added to the SDN List several individuals and entities that have financially enabled the regime, including by purchasing foreign currency on the junta's behalf.

A recurring focus of speculation since the coup, however, has revolved around whether OFAC might target the state-owned energy company ***Myanma Oil and Gas Enterprise*** ("MOGE"), which represents the largest single source of revenue for the military regime and is a critical supplier of energy for Myanmar's civilian sector as well as the economies of several states in Southeast Asia. After designating two MOGE directors earlier in the year, OFAC broke new ground in October 2023 by promulgating Directive 1 under E.O. 14014, which prohibits U.S. persons from providing broadly defined "financial services" to or for the benefit of MOGE. By imposing limited, sectoral sanctions—under which U.S. persons (and non-U.S. persons when engaging in a transaction with a U.S. touchpoint) are prohibited from engaging in only certain narrow types of activities with designated entities—rather than full blocking sanctions, OFAC appears to have been seeking to minimize collateral consequences for the people of Myanmar and its neighbors that would result from targeting an enterprise as large and interconnected as MOGE. Myanmar now joins a very small group of OFAC sanctions programs—presently Russia, Venezuela, and China—that feature sectoral restrictions. Following the model of those sanctions programs, it is conceivable that OFAC could in the future further restrict dealings involving Myanmar's oil and gas sector, as the Trump administration did by escalating from sectoral to full blocking sanctions on Venezuela's state-owned oil company.

D. Sudan

Since April 2023, two rival military factions in Sudan—the Sudan Armed Forces and the Rapid Support Forces—have waged a brutal civil war that has led to thousands of casualties and displaced millions of people both inside Sudan and outside the country. Following the outbreak of fighting, President Biden in May 2023 issued Executive Order 14098, which authorizes OFAC to impose blocking sanctions on individuals and entities deemed responsible for undermining Sudan's democratic transition or exacerbating the country's instability. OFAC to date has announced five rounds of sanctions designations pursuant to this new authority, targeting parties on both sides of the conflict, including high-ranking military and government officials for allegedly fueling the conflict in Sudan or perpetrating human rights abuses.

Crucially, despite the new Executive Order and recent additions to the SDN List, the United States has *not* re-imposed comprehensive sanctions on Sudan. Those original measures were lifted in October 2017 in response to apparent moves toward democracy. As such, the few U.S. sanctions on Sudan that remain in place principally restrict U.S. nexus dealings involving a small, but growing, number of Sudanese individuals and

entities identified on the SDN List, plus such parties' majority-owned entities. That said, in light of the politically uncertain climate and potential for further sanctions designations, businesses considering engaging with Sudan may wish to proceed with caution if such activities will involve parties closely associated with Sudan's military, intelligence, or security services.

E. Counter-Terrorism

Following the October 7, 2023 attack by Hamas terrorists on Israeli civilians, the United States has expansively used its counter-terrorism sanctions authorities to target Iran-backed militant groups.

The Biden administration has on multiple occasions imposed blocking sanctions on individuals and entities associated with Hamas. Although dealings involving Hamas itself have long been restricted by virtue of that group's designation as both a Foreign Terrorist Organization ("FTO") and a Specially Designated Global Terrorist ("SDGT"), recent actions by OFAC—often in coordination with the United Kingdom and other allied states—have chiefly targeted the organization's alleged financial facilitators. To minimize the potential collateral consequences of such designations, including the possibility that global banks could de-risk from even lawful transactions involving the Gaza Strip, OFAC in November 2023 published guidance reiterating that numerous general licenses remain available to authorize legitimate humanitarian trade in support of the Palestinian people.

Elsewhere around the region, Ansarallah (commonly known as the "Houthis")—the Iran-aligned rebel movement that exercises *de facto* control over northern Yemen—has conducted escalating drone and missile strikes targeting shipping in and around the Red Sea, ostensibly in response to Israel's ground invasion of Gaza. In addition to launching a series of coordinated airstrikes with British forces against Houthi targets in Yemen, the United States on January 17, 2024 re-named Ansarallah a Specially Designated Global Terrorist. The designation, which appears calibrated to impose tangible consequences on an armed group disrupting global shipping without exacerbating the humanitarian situation inside Yemen, is unusual and noteworthy in several key respects:

- The Houthis had recently been de-listed. Shortly after President Biden assumed office, the U.S. Department of State in February 2021 announced the lifting of the Houthis' designation as both a Foreign Terrorist Organization and a Specially Designated Global Terrorist. The Houthis were initially designated 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.
- In re-designating the Houthis in January 2024, the Biden administration deliberately named the group an SDGT—which subjects the Houthis to full blocking sanctions—without also applying the Foreign Terrorist Organization label. An FTO designation carries far more onerous restrictions, including possible criminal liability for parties that provide "material support" to such a group, that could have deterred humanitarian organizations from providing aid to Yemen.
- The Houthis' designation came with a 30-day delay, with restrictions set to take effect on February 16, 2024. U.S. blocking sanctions typically take effect immediately to minimize the risk of asset flight. The delayed effective date appears calculated to give the Houthis an opportunity and an incentive to halt their attacks on Red Sea shipping.
- OFAC issued multiple general licenses and published guidance affirming that Yemen is not now, and will not on February 16, 2024 become, subject to comprehensive sanctions—an apparent effort to provide non-governmental organizations comfort to continue providing lawful humanitarian assistance to the Yemeni people.

Whether, and for how long, the Houthis remain a designated terrorist organization will depend on the rapidly shifting security situation in Yemen as the Biden administration has, for now, left the door open to lifting sanctions on the group in the event that their attacks cease.

F. Other Major Sanctions Programs

Although Cuba, North Korea, and Syria remain subject to comprehensive U.S. sanctions—as a result of which U.S. persons are, except as authorized by OFAC, generally prohibited from engaging in transactions with a nexus to those jurisdictions—each of those sanctions programs was comparatively quiet during 2023. As of this writing, the Biden administration has not announced any new Cuba-related designations or regulatory changes in over a year. The chief sanctions development out of Syria consisted of the issuance of a since-expired general license and related guidance designed to facilitate the flow of humanitarian aid to the Syrian people following a devastating series of earthquakes in February 2023. OFAC also continued to, from time to time, designate additional parties for engaging in North Korea-related activities, including generating revenue for Pyongyang, supporting the Kim regime's weapons programs, and facilitating arms transfers from North Korea to Russia. However, any one of those three programs could quickly become more active during the coming year—including, for example, if North Korea were to conduct a nuclear test or continue to threaten an assault on South Korea.

G. Crypto/Virtual Currencies

In 2023, OFAC amplified its focus on illicit finance in the virtual currency sector through a mix of new designations to the SDN List and aggressive enforcement actions. These actions, which build on or otherwise supplement prior designations, suggest OFAC's continued willingness to target malicious cyber-actors, often in coordination with other U.S. Government agencies and increasingly agencies in allied jurisdictions.

In April 2023, OFAC designated ***Genesis Market***, one of the largest illicit marketplaces for stolen credentials and sensitive data, including email addresses, usernames and passwords, and mobile device identifiers. In parallel, the U.S. Department of Justice and counterparts abroad announced criminal enforcement actions against Genesis Market users and seized associated domain names to effectively shut down the marketplace. While Genesis Market was operational, tens of millions of dollars' worth of virtual currency was reportedly exchanged on the platform. These U.S. Government actions echo the earlier designation and takedown of ***Hydra Market***, which we describe in our 2022 Year-End Sanctions and Export Controls Update.

In August 2023, OFAC designated one of the co-founders of the virtual currency mixer ***Tornado Cash***—a platform allegedly used by the Lazarus Group, a North Korea state-sponsored hacking group, to launder hundreds of millions of dollars of stolen virtual currency. The designation was made pursuant to both cyber-related and North Korea-related sanctions authorities on the basis of providing "material support" to the already-sanctioned Tornado Cash and the Lazarus Group. In coordination, DOJ unsealed an indictment against two Tornado Cash co-founders alleging conspiracy to commit sanctions and anti-money laundering violations.

The Biden administration followed up on those actions in November 2023 by designating ***Sinbad.io*** ("Sinbad"), another virtual currency mixer known to be a "key money-laundering tool" of the Lazarus Group used for laundering millions of dollars of ill-gotten virtual currency. In particular, Sinbad was allegedly used to launder a significant portion of the $100 million in virtual currency stolen in June 2023 in a heist linked to the Lazarus Group.

These designations together suggest that OFAC continues to focus not just on financial criminals, but also the platforms, tools, software, and even algorithms used in those crimes and the creators of such technologies. Although hacking threats are dispersed throughout the globe, the North Korea-based Lazarus Group has been a recurring feature of OFAC's

cyber-related designations. It would not be unsurprising if, in coming months, OFAC were to announce additional sanctions designations aimed at further denying the Lazarus Group resources to carry out its malicious activities.

H. OFAC Enforcement Trends and Compliance Lessons

2023 was a historic year for OFAC enforcement as the agency, for the first time ever, imposed a combined $1.5 billion in civil monetary penalties. Although the number of OFAC enforcement actions resulting in monetary penalties was unexceptional—17 cases is roughly in line with the agency's long-term average—the size of those penalties was striking. In just the past year, OFAC levied two of the six largest civil penalties in its history, including a $508 million settlement with a global tobacco company and a record-breaking $968 million settlement with a leading cryptocurrency exchange.

Within OFAC's enforcement actions for 2023, a few notable trends stand out. More than half of the agency's published cases were brought against providers of financial services (6 of 17) or virtual currency services (4 of 17), both of which are likely to remain enforcement priorities during the year ahead. Moreover, multiple cases—including the two largest penalties imposed by OFAC this past year—involved parallel resolutions with DOJ (and other agencies), suggesting an increased appetite on the part of the U.S. Government for civil and *criminal* enforcement of U.S. sanctions.

We highlight below the most noteworthy compliance lessons from OFAC's 2023 enforcement actions, some of which are thematically consistent with prior years and others of which are relatively new. Many of these takeaways were explicitly communicated by OFAC, which includes a "compliance considerations" section in the web notice for each of its enforcement actions:

- **Non-U.S. companies should ensure that their activities do not "cause" U.S. persons to violate U.S. sanctions restrictions**: Per OFAC, non-U.S. companies are on notice of this obligation when they avail themselves of U.S. customers, goods, technology, or services. Four non-U.S. companies were penalized this past year for "causing" violations, with most alleged to have utilized the U.S. financial system in transactions otherwise involving non-U.S. parties—a common fact pattern in recent years. Despite criticisms of the arguably extraterritorial reach of actions like these, OFAC has not been shy about bringing them.
- **U.S. parent companies should take steps to ensure that their non-U.S. subsidiaries comply with applicable sanctions restrictions**: OFAC has repeatedly recommended that multinational enterprises assess the sanctions risks of their foreign subsidiaries, particularly those operating in high-risk jurisdictions. The agency has cautioned against pursuing new business overseas without setting up proper compliance controls such as policies for U.S. person directors, officers, and employees to recuse themselves from prohibited activities and whistleblower programs to identify prohibited conduct.
- **Restricted party screening protocols should utilize all available relevant information**: In at least six enforcement actions in 2023, across economic sectors, OFAC highlighted the importance of reviewing counterparties' identifying information both at the outset of the business relationship and on a recurring basis thereafter. If available, location-related information and documentation—such as Internet Protocol ("IP") addresses, top-level domains, passports, and customer-provided addresses—is key to effective restricted party screening.
- **Virtual currency companies should incorporate risk-based sanctions compliance at an early stage**: OFAC has said that it expects compliance from "day one," even where a company may still be establishing itself and developing its product offerings. Moreover, companies are responsible for ensuring the sanctions compliance of the technologies, software, and platforms that they employ, even if those technologies are "autonomous." This has ramifications not only for virtual

currency companies, but also startups working with artificial intelligence and other emerging technologies. OFAC clearly showed in 2023 how active it can be in policing the sanctions compliance of virtual currency companies, and so it may surprise some observers that the agency has asked Congress to significantly expand and clarify its enforcement authority in the virtual currency space.

- **Companies should remain vigilant for efforts by persons in Russia and Russian-occupied regions of Ukraine to evade sanctions**: Almost half of OFAC's published cases in 2023 alleged violations of its Ukraine- and Russia-related sanctions (7 of 17)—a much higher percentage than in the years preceding Russia's full-scale invasion of Ukraine. As the war persists, we expect to see many more Russia-related enforcement actions.

In sum, OFAC has adopted an extraordinarily aggressive posture in a number of areas that could portend a return to the nine-figure penalties that defined sanctions enforcement for much of the last decade.

IV. U.S. Export Controls

As made evident through U.S. policy toward Russia and China, in 2023 export controls continued their rise as indispensable and central tools to further broader U.S. national security interests. A key part of this strategy involved coordinating controls with close allies and partners.

A. Multilateral Coordination

1. Export Controls and Human Rights

In March 2023, the United States and partner countries released the Code of Conduct for the Export Controls and Human Rights Initiative, which was founded during the Summit for Democracy in 2021 to create a framework for coordinated export controls to advance human rights. As we describe in an earlier client alert, the Code of Conduct calls for subscribing states to consider human rights as a crucial part of the effective application of export controls, consult with regulated parties, and cooperate with other subscribing states on this front.

Together with the announcement of the Code of Conduct, the U.S. Department of Commerce published a final rule explicitly confirming that human rights abuses worldwide can be a basis for adding parties to the Entity List. Concurrently therewith, BIS added to the Entity List 11 entities based in Myanmar, China, Nicaragua, and Russia for their alleged involvement in human rights abuses such as suppressing peaceful protests with surveillance technology or conducting aerial attacks on civilians.

While the Export Controls and Human Rights Initiative was initially founded by the United States, Australia, Denmark, and Norway, 21 more countries joined to endorse the voluntary Code of Conduct upon its release—Albania, Bulgaria, Canada, Costa Rica, Croatia, Czechia, Ecuador, Estonia, Finland, France, Germany, Japan, Kosovo, Latvia, the Netherlands, New Zealand, North Macedonia, the Republic of Korea, Slovakia, Spain, and the United Kingdom. Many of these countries were already closely coordinating regarding trade controls resulting from the war in Ukraine.

These 25 subscribing states gathered in Washington, D.C. again in September 2023 for the inaugural plenary hosted by the U.S. Department of State. While highlighting the various trade controls tools that the United States is already employing to counter human rights violations and abuses, senior U.S. officials acknowledged that "the United States cannot confront the issue of dual-use tech being used to commit [human rights] abuses alone." With the collaborative momentum and experience gained from developing and implementing Russia-related sanctions and export controls, we are likely to see increasing global cooperation on human rights-related controls, including on surveillance

technologies or other items used for arbitrary arrest, detention, and/or suppression of peaceful protests.

2. Allies, Partners, and Incentives

Cooperation on human rights is just one example of the growing importance of multilateralism as a core tenet of U.S. trade controls policy. Another example can be found in the June 2023 formal agreement among the Five Eyes partners—Australia, Canada, New Zealand, the United Kingdom, and the United States—to coordinate on export control enforcement.

To further strengthen these global ties and partnerships, BIS on December 8, 2023, issued three separate rules amending the EAR to liberalize export licensing requirements to certain countries that are allies of the United States or members of multilateral export control regimes.

In the first final rule, BIS made two changes to eliminate licensing requirements for exports to certain friendly countries. First, BIS removed Proliferation of Chemical and Biological Weapons ("CB") controls on specified pathogens and toxins that are destined for the 43 Australia Group member countries—a forum that is potentially ripe for further export controls coordination as Russia is not a member. Items affected by this change are now controlled under CB Column 2, which does not require a license for exports to Australia Group member countries, instead of CB Column 1. Second, BIS removed Crime Control and Detection ("CC") controls on certain items that are destined for Austria, Finland, Ireland, Liechtenstein, South Korea, Sweden, and Switzerland. Items affected by this change are controlled under CC Column 1 and Column 3, which no longer result in license requirements for these seven allied countries.

In the second final rule, BIS expanded license exception eligibility for Missile Technology ("MT") controlled items to resolve certain domestic inefficiencies and harmonize controls with other Missile Technology Control Regime member countries. With this change, exporters may rely on license exceptions Temporary Imports, Exports, Reexports, and Transfers ("TMP"), Governments ("GOV"), and Technology and Software - Unrestricted ("TSU") for MT-controlled items subject to the specific terms and conditions specified in the relevant regulations, and may rely on license exception Aircraft, Vessels, and Spacecraft ("AVS") for additional ECCNs.

In a third proposed rule, BIS proposed changes to license exception Strategic Trade Authorization ("STA") to encourage its use by allied and partner countries. As part of the proposed rule, BIS raised several questions for public comment, including "[w]hat additional changes could be made to License Exception STA to further facilitate exports, reexports, and transfers (in-country) between and among destinations identified in both Country Group A:5 in supplement no. 1 to part 740 and supplement no. 3 to part 746." BIS received comments on the proposed rule through February 6, 2024, and will likely issue a final rule based on public feedback.

In all three rules, BIS emphasized the importance of multilateral and plurilateral export controls, which the agency described as "the most effective path toward accomplishing our national security and foreign policy objectives." These changes demonstrate continuing efforts by the U.S. Government at fostering global coalitions around export controls implementation and enforcement and creating incentives for more countries to join the alliance.

B. Commerce Department

1. Disruptive Technology Strike Force

Under the Biden administration, BIS has prioritized regulations that restrict the flow of advanced technology to U.S. adversaries. In a continuation of this regulatory priority, the

Department of Justice's National Security Division and the Department of Commerce's BIS in February 2023 launched the Disruptive Technology Strike Force to protect certain advanced U.S. technologies from being illegally acquired and used by nation-state adversaries such as Russia, China, and Iran. The Disruptive Technology Strike Force includes experts throughout government—including the Federal Bureau of Investigation, Homeland Security Investigations, and more than a dozen U.S. Attorneys' Offices.

According to U.S. Deputy Attorney General Lisa O. Monaco, the Strike Force's mandate is to restrict adversaries' abilities to acquire, use, and/or abuse innovative U.S. technology to "enhance their military capabilities, support mass surveillance programs that enable human rights abuses and all together undermine our values." The Strike Force specifically targets technology related to supercomputing and exascale computing, artificial intelligence, advanced manufacturing equipment and materials, quantum computing, and biosciences—which technologies can be used to improve calculations in weapons design and testing; improve the speed and accuracy of military or intelligence decision-making; and break or develop unbreakable encryption algorithms that protect sensitive communications and classified information.

Within its first year, the Strike Force's efforts have already led to five indictments in connection with efforts to provide materials, trade secrets, and items for military capabilities in Russia, China, and Iran; three temporary denial orders ("TDOs"); and 42 new Entity Listings.

The establishment of the Disruptive Technology Strike Force suggests an ongoing commitment to maintaining the United States' technological edge over its adversaries and reflects a bipartisan trend of aggressively utilizing export controls to pursue policy and national security goals. The Strike Force's ability to investigate violations and impose criminal and administrative penalties increases the potential risk of non-compliance. As such, companies involved in the design, production, or export of "disruptive" technologies subject to U.S. jurisdiction should closely monitor their end users and end uses.

2. Updated Voluntary Self-Disclosure Policy

Throughout 2023 and early 2024, BIS continued to refine and calibrate its approach to voluntary self-disclosures of possible violations of the Export Administration Regulations.

BIS implemented a transformative policy shift in a June 2022 memorandum that introduced a 60-day "fast track" review for voluntary self-disclosures of minor or technical infractions, while reserving a more comprehensive review for significant possible violations of the EAR. In April 2023, BIS further clarified its stance in a new agency memorandum (the "2023 EAR Enforcement Memo") allowing parties to bundle multiple voluntary self-disclosures for minor or technical infractions into one overarching submission. As discussed below, BIS subsequently clarified that bundled self-disclosures for minor or technical infractions may be submitted quarterly.

BIS also announced in the 2023 EAR Enforcement Memo that a *failure* to disclose significant violations will now be treated as an aggravating factor, thereby heightening the incentives for entities to voluntarily disclose and emphasizing the importance of an effective compliance program. This is a significant departure from past practice. Previously, BIS treated voluntary self-disclosures of possible violations as a mitigating factor in assessing penalties, but a failure to submit was treated in a neutral manner. Under the new policy, when an export control violation reflects potential national security harms, it will be treated as an aggravating factor under the agency's enforcement guidelines. This is in part because BIS considers a failure to disclose as indicative of the inadequacy of a corporate compliance program, which is itself a factor under BIS's settlement guidelines. In another major departure, the 2023 EAR Enforcement Memo also incentivizes parties to disclose possible export control violations by *other* parties by clarifying that a track record of cooperation, including as part of a third-party disclosure, could be considered a mitigating factor should the disclosing party be

investigated for a future, even unrelated, enforcement action. Together, the clarified policy of the 2023 EAR Enforcement Memo is intended to encourage parties to voluntarily disclose possible violations.

Since implementing the above-described changes, BIS reports that it received 80 percent more voluntary self-disclosures containing potentially serious violations during fiscal year 2023 than in the prior fiscal year. Moreover, the agency reports reduced processing time for minor or technical disclosures and 33 percent more tips from third parties.

In a separate memorandum released on January 16, 2024, BIS announced four new enhancements to the agency's voluntary self-disclosure program intended to further streamline the preparation and review of voluntary self-disclosures. First, as previewed above, the new enhancements clarified BIS's allowance of bundled disclosures of minor or technical infractions to allow parties to submit this bundle quarterly. Second, the agency decreased submitting parties' diligence burden in two ways: (1) BIS now requests that parties submit abbreviated narrative accounts of the violation in lieu of the more onerous supporting documentation listed in Section 764.5(c)(4) of the EAR, unless specifically requested by BIS's Office of Export Enforcement ("OEE"); and (2) BIS no longer requires the five-year lookback period recommended in Section 764.5(c)(3) of the EAR. Third, BIS strongly encourages submission of voluntary self-disclosures via email. Last, BIS and OEE will expedite requests for corrective action that would otherwise be prohibited by Section 764.5(f) of the EAR, and specifically invites parties to request permission to engage in such corrective action even if they are not submitting a voluntary self-disclosure. These enhancements are designed to help BIS and regulated parties prioritize their compliance resources on significant violations and to take quick corrective action where appropriate.

3. BIS Enforcement Trends

OFAC was not alone in bringing record-breaking enforcement actions during 2023. BIS in April 2023 announced a $300 million civil penalty against two affiliates of a global technology company for allegedly selling hard disk drives to ***Huawei Technologies Co. Ltd.*** ("Huawei") in violation of U.S. export controls. This enforcement action is not only the largest standalone administrative penalty in the agency's history, but also the first action targeting an alleged violation of the Huawei-specific Foreign Direct Product Rule—a notoriously complex regulatory provision that expands the scope of U.S. export controls to certain foreign-produced items that are derivative of specified U.S. software and technology.

Moreover, BIS enforcement activity was not limited to one major case. The agency over the course of 2023 secured an all-time number of convictions, temporary denial orders, and post-conviction denial orders. In a sign of the aggressiveness of BIS enforcement, the agency in early 2024, in an unprecedented move, announced a $15 million bounty on an Iranian national accused of violating U.S. export controls by procuring for Iran's Islamic Revolutionary Guard Corps goods and technology used in attack UAVs that were subsequently sold to Russia.

In light of increasing U.S. export enforcement risks, even companies outside of the United States should carefully analyze the potential applicability of U.S. export controls with the broad jurisdictional reach of provisions like the Foreign Direct Product Rule in mind.

4. Extended Renewal Period of Temporary Denial Orders

When BIS determines that an individual or entity presents an imminent risk of violating the EAR or has been convicted of violating certain U.S. laws and regulations—including U.S. sanctions and export control laws and regulations—BIS may issue an order denying that person export privileges. The effect of a denial order is that the targeted person is typically prohibited from participating in any way in any transaction involving items subject to the EAR, including both exporting from the United States and receiving or benefiting

from any export, reexport, or transfer of any item subject to the EAR.

Depending upon the circumstances, BIS may issue one of two types of denial orders. BIS may issue a temporary denial order, which historically has been renewable for multiple periods of up to 180 days, upon a determination that such an order is necessary to prevent an imminent violation of the EAR. Alternatively, upon a determination that any person has been convicted of violating certain specified U.S. statutes or any regulations issued pursuant thereto (including the EAR or OFAC's sanctions regulations), BIS may issue a denial order for a period of up to ten years from the date of conviction. As noted above, a denial order—which results in the target being added to the Denied Persons List—is an especially powerful tool as it completely severs a non-U.S. person's access to the U.S. supply chain.

In August 2023, BIS amended Section 766.24(d)(1) of the EAR, creating an additional ability to renew an existing temporary denial order for one year under certain conditions. While maintaining BIS's ability to renew an existing TDO for 180 days if "the denial order is necessary in the public interest to prevent an imminent violation," the amendment adds the ability to specify an extended renewal period of one year upon a showing that the party subject to the TDO has engaged in a pattern of repeated, ongoing, and/or continuous apparent violations of the EAR, and that the extended renewal is appropriate to address such continued apparent violations.

In its final rule, BIS offered three examples of circumstances under which an extended renewal would be appropriate. Namely, if the respondent has:

- Acted in apparent blatant disregard of the EAR;
- Attempted to circumvent or otherwise appeared to violate the restrictions of a TDO or the EAR; or
- Otherwise acted in a manner demonstrating a pattern of apparent noncompliance with the requirements of the EAR.

BIS specifically identified repeat offenders of Russia-related controls as the type of cases in which extended renewals would serve as an enhanced deterrent to potential offenders and enhanced notice to companies and individuals wishing to do business with the subjects of the TDO.

5. Antiboycott Enforcement Policy

In our 2022 Year-End Sanctions and Export Controls Update, we highlighted BIS's intensified enforcement approach toward U.S. antiboycott regulations, marked by significant adjustments to violation categories. This past year, BIS continued to enhance its enforcement posture with respect to the antiboycott regulations, especially concerning the Arab League Boycott of Israel. In 2023, BIS imposed over $425,000 in penalties on companies for alleged violations of the antiboycott regulations.

In an agency memorandum issued in July 2023, BIS announced that the agency has amended its Boycott Request Reporting Form to require the filer to specify the party who made the boycott-related request and published an Antiboycott Policy Statement on the Department of Commerce's Office of Acquisition Management website for government contractors. In light of the enhanced regulations and enforcement priorities, U.S. firms with potential foreign boycott exposure should consider implementing robust policies to ensure antiboycott compliance.

V. Committee on Foreign Investment in the United States (CFIUS)

In addition to sanctions and export controls, the Committee on Foreign Investment in the United States—the interagency committee tasked with reviewing the national security risks associated with foreign investments in U.S. companies—remained active during 2023 as

the Committee reviewed a record number of filings and continued to closely scrutinize China-related deals. Over the past year, CFIUS also expanded its jurisdiction to include additional military installations, competed with state-level restrictions on foreign investment, increased scrutiny of deals involving Japanese and Middle Eastern investors, and prepared to operate alongside a brand new *outbound* investment review mechanism unveiled by the United States.

A. CFIUS Annual Report

In July 2023, CFIUS published its annual report to Congress detailing the Committee's activity during calendar year 2022 (the "CFIUS Annual Report"). As noted in a prior client alert, our key takeaways from the CFIUS Annual Report include:

- While the total number of filings before CFIUS largely stayed on pace with 2021, with the Committee reviewing a total of 440 filings (compared to 436 filings in 2021), the CFIUS Annual Report data may suggest a significant *proportional increase* in CFIUS filings in light of significantly slower mergers and acquisitions activity and decreased foreign direct investment in 2022;
- Declaration filings jumped 30 percent from 2020 to 2021, but decreased by approximately 6 percent in 2022, possibly suggesting a growing hesitation in the market to use the Committee's short-form declaration process;
- More than 50 percent of all non-real estate notices reviewed by the Committee were transactions in the finance, information, and services sector, signaling that transactions wherein sensitive personal data is very likely to be at issue continue to account for a large portion of the Committee's caseload (and will likely continue to do so going forward); and
- A 67 percent increase from 2021 in instances where the Committee adopted mitigation measures and conditions to mitigate the national security risks associated with a transaction, combined with an uptick in withdrawn notices, may suggest that the Committee is taking a more aggressive stance on imposing conditions on its approvals.

B. Expanded Jurisdiction

In May 2023, the Committee published two new frequently asked questions ("FAQs") that have had substantial impacts on parties notifying the Committee of a transaction. The first FAQ clarified CFIUS's interpretation of the "completion date" for a transaction, effectively negating the use of "springing rights" for mandatory filings. The second FAQ confirms that CFIUS can request certain information from passive investors, including limited partners in an investment fund.

Under 31 C.F.R. § 800.206, the term "completion date," with respect to a transaction, is the earliest date upon which any ownership interest, including a contingent equity interest, is conveyed, assigned, delivered, or otherwise transferred to a person, or a change in rights that could result in a covered control transaction or covered investment occurs. In the first FAQ, the Committee explained that, in a transaction where the ownership interest is conveyed before the foreign person receives the corresponding rights, the "completion date" is the earliest date upon which the foreign person acquired any of the equity interest. For example, if Company A acquired a 25 percent ownership interest in Company B on July 1, but its right to control Company B was deferred until after CFIUS reviews the transaction, the "completion date" for the transaction is July 1. Using this example, the Committee indicated that if the transaction is subject to the mandatory declaration requirement pursuant to 31 C.F.R. § 800.401, the latest date that the parties can file the transaction with CFIUS is June 1.

In practice, the first FAQ means that parties can no longer use a springing rights strategy to delay the onset of a mandatory CFIUS filing because CFIUS no longer distinguishes

between initial passive equity investments and future CFIUS triggering rights. In other words, parties may not delay submitting a mandatory filing by deferring acquisition of control, governance, or information access rights, while otherwise closing the investment. Parties have frequently utilized this strategy as a means to ensure the quick exchange of capital for equity interests that transfer upon execution of the transaction documents. Now, this strategy is no longer workable, as parties must submit a mandatory filing no later than 30 days prior to the transfer of the initial passive equity interest, even if the parties have negotiated a different structure.

The practical effect of the second FAQ is that the Committee may request information on *all* foreign investors involved, directly or indirectly, in a transaction, including limited partners that have passively invested in an investment fund at any level, regardless of any confidentiality provisions or contract arrangements between the limited partners and the foreign investor. Parties before the Committee have typically disclosed limited partners with five percent or more ownership and/or non-customary rights. However, this FAQ may change that approach. Going forward, on a case-by-case basis, we expect the Committee to consider the nationality, identity, and capabilities of *limited* partners. In particular, the FAQ explains that CFIUS may request identifying information for indirect foreign person investors, their jurisdiction(s) of organization, and information with respect to any governance rights and other contractual rights that investors collectively or individually may have in an indirect or direct acquirer or the U.S. business to facilitate the Committee's review regarding jurisdictional or national security risk-related considerations.

Proximity to sensitive U.S. military installations and properties is an important element of the Committee's review over certain covered real estate transactions. Specifically, the Committee has jurisdiction to review certain purchases or leases by, or concessions to, a foreign person of real estate in close proximity (the area that extends outward one mile from the boundary of the military installation or facility) to, or the extended range of (within a 100-mile radius), specific military installations and properties listed at Parts 1 and 2 of Appendix A to Part 802 of the Committee's regulations ("Appendix A").

In August 2023, the Committee released a final rule adding eight new military installations to Part 2 of Appendix A, which became effective September 22, 2023. The eight additional military installations include:

- Air Force Plant 42, located in Palmdale, California;
- Dyess Air Force Base, located in Abilene, Texas;
- Ellsworth Air Force Base, located in Box Elder, South Dakota;
- Grand Forks Air Force Base, located in Grand Forks, North Dakota;
- Iowa National Guard Joint Force Headquarters, located in Des Moines, Iowa;
- Lackland Air Force Base, located in San Antonio, Texas;
- Laughlin Air Force Base, located in Del Rio, Texas; and
- Luke Air Force Base, located in Glendale, Arizona.

Importantly, many military installations have been renamed, and CFIUS's Geographic Reference Tool is not always updated. Thus, parties should carefully cross-reference the names of military installations when conducting any proximity analysis.

The new rule followed shortly after the Committee determined that it did not have jurisdiction over the proposed purchase by ***Fufeng Group Limited*** ("Fufeng"), a Chinese company, of a 370-acre site in North Dakota located approximately 12 miles from Grand Forks Air Force Base. That proposed purchase faced significant political backlash and was ultimately terminated by local officials. We expect CFIUS will continue to expand the list of sensitive facilities going forward, so transaction parties should closely watch for

future additions to Appendix A.

C. State Law Investment Restrictions

Following the Fufeng controversy, U.S. states have quickly begun passing their own laws impacting real estate transactions within their borders. For example, in May 2023, Florida passed a law barring foreign principals from "countries of concern" (including China, Russia, Iran, North Korea, Venezuela, and Syria) from acquiring an interest in agricultural property or property near sensitive military sites. More than 20 states have adopted legislation restricting foreign ownership of U.S. land, and actions to amend or enact such legislation are pending in many other states.

As we discuss in a prior client alert, state laws vary in their approaches to address the potential national security and economic implications of foreign ownership of U.S. land. Some states mandate disclosure of foreign ownership of U.S. land, while other states directly prohibit certain transactions and may require divestiture of foreign-owned land. Additionally, laws differ as to who is subject to the restrictions, with some legislation seeking to regulate real property transactions with individuals and entities from a list of named countries, and other legislation seeking to govern purchases by all non-U.S. citizens.

The constitutionality of these laws remains uncertain. A group of Chinese citizens and lawful residents of Florida and a Florida corporation challenged Florida's new law under several federal statutes, including the Fair Housing Act. The U.S. Department of Justice has filed a statement of interest in the case supporting the plaintiffs' motion for a preliminary injunction and arguing that the Fair Housing Act preempts Florida's law.

More than a dozen bills have been introduced in the U.S. Congress to address concerns about foreign acquisitions of U.S. real estate. Some bills would expand federal reporting requirements in connection with foreign investments in agricultural land and increase penalties for nondisclosure. Other bills would expand CFIUS jurisdiction to encompass more categories of land, such as certain foreign investments in agricultural land and in U.S. businesses engaged in agriculture or biotechnology related to agriculture.

The state measures described above add another complex layer to the various U.S. restrictions at the federal level targeting trade and financial flows with China (and, in some cases, several other challenging jurisdictions). International investors and multinational businesses now must consider not only federal law when undertaking transactions in the United States, but must also factor in state-specific restrictions that may play an increasingly important role in managing their commercial engagements and exposure in the country.

D. Geographic Focus

In 2024, parties should expect the Committee to heavily scrutinize investments by foreign investors with ties to China. This is perhaps not surprising amid increased geopolitical tensions between Washington and Beijing.

Notably, CFIUS has increased its scrutiny of transactions involving Middle Eastern investors, especially under circumstances in which such investors have close business ties to China. Close examinations of Japanese investors' relationships with Chinese shareholders have also contributed to lengthier investigation timelines.

Due to the Committee's focus on third-party risk from China, parties should carefully consider the structure of investments. For example, there is an exception to mandatory filing requirements for investment funds managed exclusively by general partners that are not foreign persons, so long as the foreign limited partners are sufficiently passive. At bottom, companies with extensive links to China, including companies with a large Chinese customer base, should expect a thorough and rigorous review by the Committee.

VI. U.S. Outbound Investment Restrictions

While CFIUS review of *inbound* investments into the United States has been a feature of U.S. trade controls for decades, the Biden administration during 2023 laid the foundation for unprecedented *outbound* restrictions on how U.S. persons deploy capital abroad. Momentum for such a regime appears to have been driven in part by concerns among U.S. officials at the prospect of U.S. investors financing or otherwise enabling efforts by strategic competitors such as China to develop critical technologies within their own borders. Although the regulations are still under development as officials review public comments and debate how to tailor any such regime to avoid unduly restricting investments that present little risk to U.S. national security, developments over the past few months suggest that the United States could soon stand up an entirely new outbound investment review mechanism.

A. Proposed Rulemaking

On August 9, 2023, President Biden issued Executive Order 14105 authorizing restrictions on certain forms of outbound investment in semiconductors and microelectronics, quantum information technologies, and artificial intelligence systems. While the Executive Order did not immediately impose new legal obligations on outbound investments, it was accompanied by an Advance Notice of Proposed Rulemaking issued by the U.S. Department of the Treasury, the agency tasked with primary implementation authority for the Executive Order. The ANPRM provides further details about the contours of the planned requirements and restrictions. In terms of timing, the ANPRM formally began the rulemaking process by seeking significant public input to assist Treasury in crafting the final text of the regulations.

The proposed new restrictions largely track reports that the Biden administration would focus on a narrow set of high-technology sectors, imposing an outright ban on a small set of transactions and requiring notification to the U.S. Government on a broader set of others. Specifically, E.O. 14105 focuses on direct and indirect investments by "U.S. persons" in a "covered foreign person," which those measures define to consist of Chinese, Hong Kong, and Macau entities engaged in the business of targeted "national security technologies and products," which terms are still in the process of being defined.

Importantly, the proposed outbound investment regime is *not* a "catch and release" program, and in contrast to the mandatory filing requirements under CFIUS, the Treasury Department has clearly stated in the ANPRM that it is "not considering a case-by-case determination on an individual transaction basis as to whether the transaction is prohibited, must be notified, or is not subject to the program." It will not be a "reverse CFIUS." Rather, the onus will be on the parties to a given transaction to determine whether the prohibitions or notification requirements apply.

While unique, the proposed outbound rules draw on existing regulatory regimes such as export controls on software and technology, sanctions programs restricting transactions with specific parties or geographies, and inbound foreign direct investment controls under CFIUS. A novel feature of the proposed outbound regime, however, is its specific targeting of U.S. capital and intangible benefits—identified in the ANPRM as "managerial assistance, access to investment and talent networks, market access, and enhanced access to additional financing"—that often accompany investments in high-technology sectors of the Chinese economy, and which are perceived as threats to U.S. national security.

While E.O. 14105 envisions both civil and criminal penalties for violations of the proposed regulations, the ANPRM focuses on civil penalties, as is standard, with potential criminal conduct being referred to the U.S. Department of Justice. The ANPRM proposes imposing civil penalties up to the maximum allowed under the International Emergency Economic Powers Act, currently over $350,000 per violation.

B. Public Comments and Unresolved Issues

It will likely be some time before the final U.S. outbound investment rules take shape. Although the ANPRM provides useful insight into the likely scope and scale of the final regulations, it also requested comments from the public on 83 specific questions—the answers to which remain unsettled. Treasury's public comment period for the ANPRM closed on September 28, 2023.

The comment period generated significant interest from industries that will be affected by the potential outbound investment regime, with input from major actors in the investment community; manufacturers; semiconductor, microelectronics, and quantum companies; financial institutions; and trade associations. As we discuss in more detail in a separate client alert, commenters from across industries emphasized the need for more clarity, narrower coverage to prevent chilling investment and spillover into non-targeted industries, and wider exemptions.

Specifically, many commenters noted that the contemplated definitions are vague with respect to which U.S. actors or investors, foreign partners, and types of investments and transactions are subject to the restrictions. Commenters also overwhelmingly requested clear steps and extensive guidance to make it easier for investors to comply, in addition to requests for other details on how compliance standards will be applied. Finally, commenters sought to clarify the Treasury Department's proposed covered transactions and expand exemptions to prevent overbroad coverage. In particular, commenters sought to ensure that passive investments by both limited partners and non-limited partners, venture capital and private equity investments, and other transactions are not covered by the regulations. Major financial institutions and investment commenters urged the Treasury Department to clarify that coverage does not indiscriminately restrict services provided by financial institutions to their customers with respect to covered transactions.

In addition to the public comments described above, the proposed outbound investment regime has drawn opposition from prominent members of Congress. Critics of the proposal in its current form include the influential chairman of the House Financial Services Committee who, in a letter to Treasury Secretary Janet Yellen, questioned the Biden administration's policy of decreasing U.S.-driven investment in China, arguing that public policy should instead be to increase private U.S. investment and control of Chinese entities. The chairman further questioned whether the program should be administered by OFAC, rather than through the CFIUS regime. These criticisms are significant because they may identify grounds for parties to challenge the final regulations and because they highlight a sharp disagreement in the top levels of government regarding the role of U.S. investment in China.

The Biden administration appears to have expended considerable effort engaging with U.S. allies concerning the scope of the proposed restrictions, with the result that new outbound investment regimes appear to be gaining traction in jurisdictions such as the European Union. Ahead of the eventual publication of final regulations in the United States, the Biden administration is expected to continue engaging with Congressional leadership and global allies on these issues, as well as assessing the public comments it has received from business industry leaders and practitioners. Although an exact timeline for publication of a final rule has not been set, it is possible that a new U.S. outbound investment regime could take effect in the coming year.

VII. European Union

A. Trade Controls on China

Departing from the trend in recent years of skirting around China policy, a March 2023 speech by European Commission President Ursula von der Leyen assertively set the tone for EU-China relations going forward. Amid a ballooning EU-China trade deficit, von der Leyen called out China's calculated attempt at subverting the international order through

the deliberate creation of economic dependencies and the extortive use of economic leverage, as well as China's positioning as a global peace-breaker—supporting Tehran and Moscow, ramping up its military posture, and spreading disinformation. Von der Leyen further noted that China has clearly moved on from an era of "reform and opening" toward a new era of "security and control" no longer governed by the logic of free markets and open trade. Despite these remarks, von der Leyen noted the interconnectedness between the European and Chinese economies and, in a nod to U.S. nomenclature on the subject, concluded that the European Union should focus on *de-risking* from China, rather than *de-coupling*.

Tangible action followed throughout the year. In response to surging, government-assisted Chinese electric vehicles exports, the European Union launched an *ex officio* anti-subsidy investigation into the import of Chinese-manufactured EVs. As the European Commission, the bloc's executive branch, has already found evidence of support by state actors at preferential terms, the imposition of tariffs, along with corresponding Chinese retaliatory measures, appears to be a distinct possibility as a result of the investigation. The European Union has historically been more comfortable deploying trade defense measures such as tariffs and anti-dumping or countervailing duties on China, as opposed to trade or financial sanctions measures. However, while the European Union has yet to implement any particularly impactful sanctions measures as it continues to lack a China-related sanctions program, this year it reportedly considered blacklisting eight Chinese companies it had found to be assisting Russia's military operations in Ukraine. While the measures ultimately failed to rally the support of all EU Member States (which is required for such measures), the Commission's bold move to put these listings on the European Council's agenda is noteworthy. Following these developments, European Council chief Charles Michel during a year-end visit presented China's President Xi Jinping with a list of Chinese companies that may soon become subject to EU sanctions unless exports of dual-use items to Russia are addressed. As global tensions rise, appetite for EU-wide sanctions measures targeting China-based bad actors is likely to increase.

In terms of legislative initiatives, the European Union in September 2023 implemented its own Chips Act, which is designed to leverage private-public partnerships in order to onshore semiconductor manufacturing. In November 2023, the European Council and Parliament reached provisional agreement on the proposed Critical Raw Materials Act, which was first unveiled in March 2023 and aims to ensure that not more than 65 percent of EU consumption of identified strategic raw materials comes from a single third country. The European Union also continued to develop EU-wide forced labor legislation. As the post-UFLPA Chinese redirection of solar panels and related products into the European Union intensifies, Europe's prospects for a UFLPA-like "rebuttable presumption" that goods are made with slave labor have improved. In October 2023, the Internal Market and International Trade committees amended the Commission's proposed draft of the EU Forced Labor Import Ban and tasked the Commission with creating a list of geographic areas and economic sectors at high risk of using forced labor, in relation to which the burden of proof would shift to companies—rather than enforcing authorities—to demonstrate that items have not been produced with forced labor. Finally, the Anti-Coercion Instrument—a regulation enabling the Commission to take proportionate countermeasures to induce the cessation of economic coercion levied at the European Union or one of its Member States—entered into force in December 2023. While none of these initiatives explicitly mentions China, *all* form part of Europe's China strategy and indeed many were implemented in direct response to certain Chinese actions.

The most comprehensive expression of the Commission's vision for a more resilient Europe came with the publication, together with the EU High Representative for Foreign Affairs and Security Policy, of a communication to the European Parliament, the European Council, and the Council on a new European Economic Security Strategy. This communication laid the groundwork for a discussion among EU Member States and various EU institutions with a view to creating a common framework designed to minimize risks stemming from increased geopolitical tensions and accelerated technological shifts,

while preserving maximum levels of economic openness. While the communication—in keeping with European tradition—also does not mention China, it echoes von der Leyen's speech earlier in the year and points to economic security risks related to the resilience of supply chains, physical and cyber security of critical infrastructure, technology security and technology leakage, and the weaponization of economic dependencies and economic coercion. The strategy is multi-pronged and notably includes proposals to bolster the European Union's foreign investment screening tools, enhance cooperation among Member States in relation to dual-use export controls—including in relation to research security with respect to the development of technologies with dual-use potentials—and examine whether to adopt outbound investment controls akin to the proposed regime announced by the United States. As China-EU trade tensions are poised to continue into 2024, the European Union is likely to maintain an assertive economic security posture. Further details on the European Economic Security Strategy are expected in early 2024.

B. Sanctions Developments

1. Institutional and Procedural Developments within the European Union

The European Union and its Member States continued to make unprecedented progress toward harmonizing European sanctions enforcement. Such harmonization is long overdue and without it effective sanctions enforcement will continue to be lacking. At present, not all EU Member States even criminalize the violation of EU sanctions and, even among those Member States that do, criminal laws on evidentiary requirements, burden of proof standards, and penalties vary substantially. The inconsistent enforcement of restrictive measures not only undermines the effectiveness of EU sanctions, but also existing legal loopholes and lack of harmonization facilitates violations and encourages the practice of forum shopping. To address these issues, European authorities took several notable steps in the direction of centralized sanctions enforcement. Crucially, in December 2023, the European Parliament and the European Council reached a provisional political agreement on the Commission's December 2022 proposal for a Directive aimed at harmonizing criminal offenses and penalties for the violation of EU restrictive measures. Once adopted, the new rules will include a list of criminal offenses related to the violation and circumvention of EU sanctions such as failing to freeze assets, providing prohibited or restricted services, or providing false information to conceal funds that should be frozen. The new rules will also establish common basic standards for penalties for both individuals and entities, including imprisonment for at least five years for certain offenses and enhanced rules on freezing of assets subject to EU sanctions. To move the proposal forward, the European Parliament and the Council will now have to formally adopt the political agreement, after which the Directive will enter into force following its publication in the Official Journal of the European Union.

As proposals for the establishment of an EU-wide sanctions enforcement authority or for an enhanced role for the European Public Prosecutor's Office have yet to gain enough momentum to translate into a Commission initiative, individual EU Member States are ramping up their domestic efforts. In Germany, the Federal Government has approved a draft Financial Crime Prevention Act (*Finanzkriminalitätsbekämpfungsgesetz*) ("FKBG"), which, if adopted by the Bundestag and the Bundesrat, will set up a new Federal Office for Fighting Financial Crime (*Bundesamt zur Bekämpfung von Finanzkriminalität*) ("BBF"). The BBF is expected to become the new agency hosting the Central Office for Sanctions Enforcement (*Zentralstelle für Sanktionsdurchsetzung*) ("ZfS") as of June 2025 in order to achieve synergies between sanctions and anti-money laundering enforcement and to improve cooperation between investigative enforcement and criminal prosecution. The ZfS has been particularly active since its creation in early 2023, with reports of more than 150 cases currently under investigation and spectacular raids in pursuit of cases. Similarly, the Latvian State Revenue Service has started more than 250 criminal proceedings for violations of EU sanctions, and Dutch authorities have imposed fines for breaches of the EU Russia sanctions regime. While the European Union has yet to establish centralized sanctions agencies akin to OFAC in the United States or the United Kingdom's Office of Financial Sanctions Implementation ("OFSI"), Eurojust and Europol

are not standing idle, having recently supported a coordinated action of the Dutch, German, Latvian, Lithuanian, and Canadian authorities against the alleged violation of sanctions on Russia.

2. Focus on Circumvention and Evasion

Having implemented a wide range of financial and trade sanctions against Russia over the last two years, the European Union is now struggling to secure Member States' support for further substantive measures. For instance, despite having significantly reduced its reliance on Russian energy imports, the European Union has not yet fully weaned itself off of Russian energy, which has frozen the bloc's potential sanctions on liquified natural gas. Facing these political and economic realities that are unlikely to resolve in the near term, European authorities are instead focusing on more attainable and politically neutral goals such as enhancing tools against sanctions circumvention and evasion. With the introduction of new powers to combat sanctions circumvention as part of its eleventh Russia sanctions package, the European Union can now restrict the sale, supply, transfer, or export of specified sanctioned goods and technology to certain third countries considered to be at high risk of being used for circumvention. While this power has not yet been used and European Commission representatives have made it clear that it is a measure of last resort (i.e., to be used only following engagement with the third countries in question), it marks a significant step in the direction of more aggressive European sanctions implementation. Measures introduced to achieve similar objectives include, among others, the introduction of a provision compelling EU exporters to contractually prohibit the re-exportation to or for use in Russia of a number of goods and technologies, a full ban on trucks with Russian trailers and semi-trailers from transporting goods to the European Union, and the simplification of crucial annexes to EU trade sanctions regulations to reduce circumvention of sanctions by misclassification of goods.

Relatedly, the European Commission published extensive guidance on the topics of circumvention and evasion to help European economic operators identify, assess, and understand possible risks. That guidance—a first on the topic—outlines due diligence best practices and includes an extensive list of circumvention red flags, which the Commission expects European economic operators to be aware of and incorporate into their risk assessments. The Commission guidance has been followed by separate guidelines at the Member State level, with Germany's Federal Ministry for Economic Affairs and Climate Action (*Bundesministerium für Wirtschaft und Klimaschutz*) ("BMWK") issuing further guidance for companies to tackle circumvention and evasion of trade sanctions. As discussed more fully above, the European Union together with its international partners published a List of Common High Priority Items intended to support compliance by exporters, and also targeted anti-circumvention actions by customs and enforcement agencies of partner countries to prevent their territories from being abused for circumvention of EU sanctions.

3. Iran Sanctions and Policy

The European Union has yet to develop a coherent and uniform stance in relation to Iran. Historically, in addition to implementing UN sanctions, the European Union imposed a wide range of autonomous economic and financial sanctions on Iran. The European Council recently decided to refrain from lifting these restrictive measures on Transition Day (i.e., October 18, 2023), as originally envisaged under the Joint Comprehensive Plan of Action.

The European Union has also reacted to Iran's support for Russia's invasion of Ukraine. In July 2023, the Council established a new framework for restrictive measures in view of Iran's provision of military support to Syria and Russia. This new regime prohibits the export from the European Union to Iran of components used in the construction and production of unmanned aerial vehicles. It also provides for travel restrictions and asset freeze measures that could be imposed against persons responsible for, supporting, or involved in Iran's UAV program. The Council made use of its designation powers to add

several Iranian individuals and entities to its asset freeze target list for undermining or threatening the territorial integrity, sovereignty, and independence of Ukraine.

Despite these actions, discontent looms among European politicians and bureaucrats, some of whom view the European Union's policy on Iran as weak. Members of the European Parliament recently criticized EU High Representative Josep Borrell's Iran policy, claiming it had failed and that it is purely symbolic. Borrell, however, suggested that the political will among all 27 EU Member States to dramatically alter the European Union's policy on Iran is currently lacking. The debate is likely to continue in coming months, as the European Union is also weighing whether to punish Iran for its support of Hamas. Germany, France, and Italy are reportedly in the process of introducing unilateral measures such as a ban on the export of components used in the production of missiles. This situation will likely continue to evolve as tensions in the Middle East rise in the wake of attacks by various Iran-backed militias, including Hamas, Hezbollah, and the Houthis.

C. Export Controls Developments

The need for coordinated action at the Union level in the area of export controls has become pressing. Authorities in EU Member States have already started taking matters into their own hands which could threaten to further splinter any pan-European approach. For example, in 2023 the U.S. Government spearheaded a significant effort to persuade the Netherlands and Japan—two countries with advanced semiconductor manufacturing equipment capabilities—to establish controls similar to the U.S. restrictions described in Section II.A.1, above. In June 2023, as part of this trilateral agreement, the Netherlands imposed export controls on advanced semiconductor production equipment bound for China. Italy, too, used its so-called "golden power" to restrict the flow of information and know-how relating to proprietary technologies to China-based ***Sinochem***, ***Pirelli***'s largest shareholder and, to crack down on circumvention of EU trade sanctions on Russia, implemented national legislation imposing a prior authorization requirement for exports of certain dual-use goods for use in aviation to Armenia, Iran, Kazakhstan, and Kyrgyzstan. Spain adopted a national control list imposing new export controls on quantum computing, additive manufacturing, and other emerging technologies for reasons of national security. As the uncoordinated proliferation of national controls by EU Member States risks creating loopholes, jeopardizing the integrity of the single market, and weakening the bloc's economic security, the European Commission is pressing for the centralized implementation of a wider set of export controls.

In light of the above and as a function of its de-risking strategy, 2023 saw the European Union take decisive steps toward bloc-wide export controls for a broad set of sensitive technologies. The Commission issued a recommendation—as a part of the European Economic Security Strategy—to conduct a risk assessment exercise aimed at identifying vulnerabilities in connection with advanced semiconductors, artificial intelligence, and quantum and bio-technologies (i.e., technology areas considered highly likely to present the most sensitive and immediate risks to technology security and leakage). Potential controls restricting the export of these four types of technologies may follow in early 2024. The wider European Economic Security Strategy also promises to address gaps in the current dual-use regulation, with a view to introducing uniform controls on a wider range of items. In the meantime, for the first time, the Commission compiled all unilaterally implemented lists.

D. Foreign Direct Investment Developments

With the publication of the European Economic Security Strategy, the Commission announced plans to revise the 2020 Foreign Direct Investment ("FDI") Screening Regulation that sets minimum requirements for Member States' FDI screening, including an expanded list of sectors and activities that will trigger a screening requirement and implementing measures to harmonize processes across Member States' regimes. Earlier in the year, the European Court of Auditors had published a special report that found "significant divergences" in Member States' screening mechanisms. 22 of 27 Member

States presently have screening mechanisms in place, and EU members have significantly increased their screening of foreign investments, formally screening more than half of all investment authorization requests. Despite the recent heightened focus on FDI screening, the EU regime, which seeks to balance the free movement of capital against national security concerns, remains less aggressive than companion regimes in the United States and the United Kingdom. EU Member States authorize the overwhelming majority of transactions without conditions and, in July 2023, the European Court of Justice conservatively interpreted the EU regime's reach, holding that screening cannot be used as a protectionist tool, as foreign investments cannot be restricted on the basis of purely economic considerations.

However, there have been recent examples of certain EU Member States taking a harder line. In October 2023, a U.S. company was forced to abandon its global takeover of a Canadian target after the French government vetoed the acquisition of two French subsidiaries under France's FDI regime. While the rationale for this decision is not public, it appears that Paris's concerns stemmed from the transaction's potential to cause the two subsidiaries—which supply parts for nuclear submarines and reactors—to become subject to U.S. export control rules, thereby threatening supply to the French market. The parties have indicated that, although a package of remedies and undertakings was offered to French authorities, such measures were not sufficient to resolve the government's concerns.

VIII. United Kingdom

A. Trade Controls on China

Although the United Kingdom continues to refine its approach to China's increasingly assertive stance in global affairs, 2023 did not see any decisive turning points. In March 2023, the UK Government released the much-anticipated "Integrated Review Refresh 2023: Responding to a More Contested and Volatile World" (the "2023 Review"), the United Kingdom's expression of its national security and foreign policy. While it had been expected that the United Kingdom would label China a "threat," the words "epoch-defining challenge" were ultimately chosen to replace the optically weaker "systemic challenge" label chosen for the previous iteration of the review. Beyond semantics, steering clear of describing China as a threat amply demonstrates the United Kingdom's continued ambivalence toward Beijing, despite being under significant pressure from core allies to revise (and strengthen) its stance. Nevertheless, the 2023 Review highlighted UK concerns with the Chinese Communist Party's conduct, specifically calling out China's strengthening of its relationship with Russia, its disregard for human rights and international commitments in Tibet, Xinjiang, and Hong Kong, the militarization of disputes in the South China Sea, China's refusal to renounce the use of force in Taiwan, the country's ruthless use of its economic power to coerce unaligned countries, and the sanctioning of British parliamentarians in an effort to undermine free speech critical of China.

While practical takeaways specifically relating to China mainly consisted of increased multilateral cooperation with core allies and enhanced investment in diplomatic efforts, the 2023 Review mentioned other tangible initiatives. The UK Government expressed a commitment to bolster the United Kingdom's economic security and pledged to publish a new strategy on supply chains and imports of technologies of strategic importance to the United Kingdom and its allies, as well as a refresh of the Critical Minerals Strategy and the creation of a new semiconductor strategy aimed at improving the resilience of semiconductor supply chains. Similar initiatives are being pursued by the United Kingdom's core allies, as described in Sections II and VII.A, above.

Despite the commitments made in the 2023 Review, the UK Parliament's Intelligence and Security Committee in July 2023 published a detailed report calling out the lack of a clear, forward-looking China strategy and the failure to deploy a whole-of-government approach when countering threats posed by China. The report highlighted the inadequacy of UK

protections against Chinese interference and Beijing's deliberate attempt at creating economic dependencies it could (and often has chosen to) weaponize. In particular, the report exposes the multifaceted nature of the intelligence threat posed by China and calls out the economic dependency risks stemming from China's deliberate use of investment activities as a platform, as evidenced by the political influence China gains from its very significant investment in the UK civil nuclear sector. Furthermore, the report found that China has increased espionage efforts in the United Kingdom, "prolifically and aggressively" collecting human intelligence, gathering information through social media, and routinely targeting current and former civil servants.

The government's response to the report was mostly defensive and stopped short of making any new commitments. Rather, it focused on the protective (though not protectionist) measures implemented so far. Among them, the National Security Act 2023 stands out. In force since December 2023, the Act is the most significant overhaul of UK national security law in over a century and directly responds to threats of espionage, foreign interference in the political process, disinformation, and cyber-attacks. Notably, the Act creates new criminal offenses of obtaining or disclosing protected information, obtaining and disclosing trade secrets, and assisting a foreign intelligence service, and also expands the scope of existing investigative powers. The offense of obtaining or disclosing trade secrets is particularly novel as it criminalizes espionage in relation to information that has existing or potential commercial, economic, or industrial value, such as a new technology developed in the United Kingdom. In a similar vein, the government also devised the new Foreign Influence Registration scheme, which will require registration of arrangements to carry out political influence activities in the United Kingdom at the direction of a foreign power. This is similar to the United States' Foreign Agents Registration Act ("FARA").

Overall, the United Kingdom continued to pursue an indirect approach to China policy, generally refraining from frontally addressing challenges. That trend is likely to continue in 2024. Examples of this quiet approach include the rejection of most license applications for companies seeking to export semiconductor technology to China, the continued use of anti-dumping measures on imports of raw materials from China, and the UK Government's £1 billion investment in the semiconductor sector which is clearly designed to compete with Beijing.

B. Sanctions Developments

1. Ownership and Control Tests

The "ownership and control" tests employed in the UK financial sanctions context were the focus of significant attention by both practitioners and the judiciary in 2023. The UK Court of Appeal's *obiter* comments in the *Boris Mints & Ors v. PJSC National Bank Trust & Anor* case generated significant confusion regarding the breadth of the concept of "control," particularly in relation to the potential influence exercised by public officials over Russian companies by virtue of their role. The decision suggested a very broad interpretation of "control" that could theoretically have included almost all Russian government ministries, state-owned enterprises, and functions. Immediately following publication of the *Mints* judgment, the Foreign, Commonwealth & Development Office ("FCDO") issued a statement noting that the FCDO—in charge of UK sanctions policy and designations—will customarily designate a public body by name when it considers that a designated official has control over such body, and further noted that there is "no presumption on the part of the Government that a private entity based in or incorporated . . . in any jurisdiction in which a public official is designated is in itself sufficient evidence to demonstrate that the relevant official exercises control over that entity." OFSI also unequivocally departed from the Court of Appeal's comments with its new guidance on public officials, published jointly with the FCDO. Indeed, a subsequent High Court judgment (*Litasco SA v. Der Mond Oil and Gas Africa*) departed from the Court of Appeal's *obiter* comments and noted that the UK control test is concerned with "an existing influence of a designated person over a relevant affair of the company . . . not a state of affairs which a designated person is in a

position to bring about." Such interpretations by the FCDO and the High Court, which align with longstanding practice, provided a welcome dose of regulatory clarity for parties seeking to comply with UK sanctions.

2. Focus on Circumvention and Evasion

Alongside its core allies, the United Kingdom during 2023 identified countering circumvention and evasion as key priorities going forward. In this regard, the most noteworthy development is the United Kingdom's increasingly frequent designation of foreign, non-Russian companies that actively participate in sanctions evasion schemes, aid Russia's war effort, and/or otherwise contribute to the destabilization of Ukraine. Some examples include the imposition of UK sanctions on United Arab Emirates-based entities using opaque corporate structures and deceptive shipping practices to facilitate trade in Russian oil above the price cap; Iranian individuals and entities involved in providing UAVs for use by the Russian military; and prominent entities such as ***Sun Ship Management*** for supporting Russian efforts to circumvent or undermine the effects of UK and allied sanctions. This trend toward designating third-country entities, which departs from the United Kingdom's historic practice, seems certain to continue and intensify during the year ahead.

3. Cross-Agency Cooperation and Multilateralism

Again following the example of its U.S. partners, 2023 also witnessed an unprecedented level of cooperation among UK government agencies in relation to the effective implementation of UK sanctions. Several departments of government are engaging in information sharing and have issued guidance and compliance notes, often jointly. Examples of pluri-seal publications include several "Red Alerts" published by the UK National Crime Agency ("NCA"), each of which was prepared in cooperation with one or more UK government agencies. For instance, a December 2023 Red Alert on Exporting High Risk Goods and a November 2023 Red Alert on Gold-Based Financial and Trade Sanctions Circumvention were issued by National Economic Crime Centre (i.e., a multi-agency unit in the NCA), OFSI, and the FCDO, working in conjunction with law enforcement and financial sector partners as part of the Joint Money Laundering Intelligence Taskforce. Recent compound settlement notices published by HM Revenue & Customs ("HMRC") in relation to breaches of UK trade sanctions on Russia have also underscored the extent of enforcement cooperation among HMRC, OFSI, the FCDO, and the NCA.

Similarly, the UK Financial Conduct Authority ("FCA") is cooperating with OFSI in relation to compliance by regulated firms, with a particular focus on systems and controls designed to mitigate the risk of breaching sanctions and facilitating evasion. Indeed, in 2023, the FCA invested significant resources to assess the sanctions compliance programs of more than 90 financial services firms and identified several areas for improvement. The FCA now expects to be notified of any self-disclosures to OFSI, and may take independent action concerning sanctions issues when it deems necessary.

UK government agencies also extensively coordinated with their counterparts in closely allied jurisdictions. Relations with OFAC remain particularly close following the 2022 launch of the OFSI-OFAC partnership (the first anniversary of which was celebrated with a joint publication reiterating the effectiveness of that collaboration), numerous joint designations (e.g., in relation to the Russia-based cybercrime gang Trickbot), publication of a joint fact sheet on Russia-related humanitarian authorizations, and frequent participation in joint engagements. The United Kingdom also continues to make use of its wider network by engaging with Group of Seven ("G7") allies to coordinate new sanctions on Russia, working with its Five Eyes partners to issue joint guidance identifying critical items used in Russian weapons systems, and signing a new accord with South Korea in relation to the joint enforcement of sanctions against North Korea. The United Kingdom's multilateral approach to sanctions implementation is expected to intensify further in 2024.

4. Enforcement Update

OFSI made use of its new enforcement disclosure power for the first time in August 2023. Pursuant to Section 149(3) of the Policing and Crime Act 2017, OFSI is now authorized to publish details of financial sanctions breaches—including details on the identity of the person committing the breach—even under circumstances in which OFSI determines that the breaches are not serious enough to justify a civil monetary penalty. OFSI's first published disclosure underscores the importance of effective sanctions policies and procedures and adequate resourcing in the field of sanctions compliance, and importantly reiterates that approaching OFSI on a voluntary basis will be treated as a mitigating factor in determining what consequence, if any, to impose.

Similar concepts were threaded throughout OFSI's guidance on enforcement and monetary penalties for breaches of financial sanctions, last updated in December 2023, which articulates the agency's due diligence expectations. While noting that there is no one-size-fits-all approach to sanctions compliance, OFSI indicated that it will consider the degree and quality of a company's due diligence if the agency ever investigates a potential violation of financial sanctions. OFSI expects to see evidence of a reasonable risk-based decision-making process, carried out in good faith. The guidance also clarifies the range of options available to OFSI, depending upon the severity of the breach. For instance, minor sanctions breaches are likely to be dealt with via a private warning letter, provided that there are no significant aggravating factors and the breach does not form part of a wider pattern. Moderate breaches are likely to be dealt with via a public disclosure without monetary penalty, and serious breaches are likely to attract monetary penalties or, in the most egregious cases, will be referred to UK law enforcement agencies for criminal investigation and potential prosecution. OFSI also reiterated that the standard of proof for civil investigations is the "balance of probabilities," meaning that a breach is more likely than not to have occurred, rather than the "beyond reasonable doubt" standard that applies in the criminal context. Finally, OFSI shed light on some non-determinative factors that the agency can consider as aggravating, including: the circumvention of any prohibitions or the facilitation of the contravention of any prohibitions; a high financial value associated with a breach; the breach's ability to harm the regime's objectives; and a regulated person's failure to meet regulatory standards.

5. Iran Sanctions and Policy Update

The United Kingdom's stance toward Iran is being reshaped as geopolitical tensions rise and Iran continues to act as a global destabilizing force. Indeed, the UK Government's 2023 Review, discussed above, included a commitment to counter, in cooperation with allies, the threat to regional and international security posed by the Iranian regime.

Ahead of Joint Comprehensive Plan of Action Transition Day (i.e., October 18, 2023), the UK Government, together with the governments of France and Germany, issued a joint statement committing to maintaining nuclear proliferation-related measures on Iran, as well as arms and missile embargoes. The statement explicitly called out Iran's refusal to return to the JCPOA and Tehran's continued expansion of its nuclear program and its stockpile of enriched uranium without any credible civilian justification.

On Transition Day, the UK Government followed up by translating former UN sanctions into UK law and, alongside 46 other countries that have endorsed the Proliferation Security Initiative, issued a joint statement affirming a commitment to implement effective measures to interdict the transfer to and from Iran of missile-related materials, including those related to UAVs; adopt streamlined procedures for the rapid exchange of relevant information concerning Iran's proliferation activities; work to strengthen relevant national legal authorities to address Iranian missile- and UAV-related issues; and take specific actions in support of interdiction efforts related to Iran's missile and UAV programs.

The United Kingdom in July 2023 announced a new Iran sanctions regime developed to respond to unprecedented threats from the Government of Iran and Iranian-backed armed

groups, including efforts to undermine peace and security across the Middle East and plots to kill individuals on UK soil. This new instrument, which took effect in December 2023, replaces the existing Iran Human Rights sanctions regulations, and enables the alignment of Iran-related sanctions regulations as far as possible. Among several designations and restrictive measures imposed, the new regime notably includes export restrictions on drone components, as well as new powers to impose transport sanctions on ships involved in contravening existing sanctions or owned or controlled by sanctioned individuals.

These developments follow the previous broadening of sanctions on Iran in relation to human rights violations and the designation of Iranian companies under the Russia sanctions regime, and aim to bring most Iran-related restrictive measures under one heading. As hostilities in the Middle East continue to escalate, the implementation of new UK restrictive measures targeting Iran in 2024 cannot be ruled out.

C. Export Controls Developments

1. Multilateral Cooperation

The United Kingdom has taken an increasingly multilateral approach to export controls in response to Russia's full-scale invasion of Ukraine and growing geopolitical challenges. In March 2023, the UK Government issued a joint statement with 10 other countries on the need for domestic and international controls of commercial spyware technology. Noting the threat to civil liberties and national security that the misuse of such technologies poses, the United Kingdom pledged to work with other democracies to share information and to prevent the export of software, equipment, and technology to end users who are likely to use them for malicious cyber activity. As discussed under Sections I.E and IV.A, above, the UK Government and its Five Eye partners also announced a joint effort in June 2023 to enforce export controls, and on multiple occasions this past year the United States, the European Union, the United Kingdom, and Japan issued and updated their common list of high-priority items deemed critical to Russia's war effort—which items may present elevated risks of export control evasion and will likely be a top enforcement priority going forward.

2. Enforcement Update

As part of its efforts to combat circumvention and evasion, the United Kingdom in December 2023 announced that it is launching a new Office of Trade Sanctions Implementation ("OTSI"), which will allocate implementation and enforcement of UK trade sanctions to a dedicated agency.

OTSI will be responsible for civil enforcement of trade sanctions, including those against Russia which have become incredibly complex and warrant the assembly of a specialist team on the government's side. The agency will operate in parallel with OFSI, which will continue to exclusively deal with financial sanctions. OTSI will issue guidance, act as a point of contact, investigate potential breaches, issue civil penalties, and refer cases to HMRC for criminal enforcement where needed.

OTSI is designed to fill a gap in UK sanctions implementation and enforcement. In light of the growing overlap between sanctions and export controls brought about by the United Kingdom's sweeping Russia-related trade restrictions, HMRC is pursuing civil enforcement of trade sanctions breaches. However, HMRC is also tasked with export control enforcement, and its resources risk being strained in the long run. Over the past year, however, this has not stopped HMRC from pursuing several civil and criminal enforcement actions. For example, in August 2023, HMRC fined a UK company £1 million for trading unlicensed goods in violation of Russia sanctions—the largest penalty for violations of Russia sanctions to date.

UK enforcement actions were not, however, limited to violations of Russia sanctions.

HMRC announced a fine of nearly £1 million for the unlicensed export of dual-use goods in May 2023, as well as several smaller settlements throughout the year for the unlicensed export of dual-use and military goods. In addition to imposing civil penalties, HMRC brought criminal enforcement actions against corporate entities. In May 2023, the agency announced that a criminal investigation into the suspected deliberate evasion of UK export controls had led to a guilty plea for an unlicensed shipment of controlled chemicals, a dual-use good.

Despite having increased the issuance of substantial fines, HMRC continues to abide by its longstanding practice not to disclose details of persons found in violation of UK export controls and trade sanctions.

D. Foreign Direct Investment Developments

Following a sustained downward trend in inbound foreign direct investment flows, the United Kingdom adopted a more permissive approach to FDI screening in 2023. The past year saw no orders blocking or unwinding transactions, and only six final orders imposing conditions on acquisitions. While China was the clear focus of most prohibitions and conditional orders in 2022, only one of the six final orders announced in 2023 involved investors linked to China. Instead, the United Kingdom in 2023 focused on issuing orders protecting military and defense assets such as transmission systems, satellite services, and naval propulsion systems regardless of the acquirer's nationality. Four of the six final orders involved acquirers from countries that have traditionally been friends or close allies of the United Kingdom, including the United States, Canada, and France, suggesting that the United Kingdom is prepared to exercise its FDI screening powers without regard to where the acquirer is based when it believes that UK national security is at stake.

As the third anniversary of the regime approaches, the UK Government called on stakeholders both inside and outside of the United Kingdom to complete an in-depth survey on UK FDI screening with an eye toward making the regime as business friendly as possible.

* * *

In short, 2023 was another extraordinarily active year in the world of trade controls. Between Russia's ongoing war in Ukraine, continuing frosty relations between Washington and Beijing, instability in the Middle East and parts of Africa and Latin America, and a rapidly approaching U.S. presidential election (as well as elections in dozens of countries around the world), we expect further seismic shifts to keep multinational enterprises occupied throughout the months ahead.

The following Gibson Dunn lawyers prepared this update: Scott Toussaint, Irene Polieri, Adam M. Smith, Stephenie Gosnell Handler, Christopher Timura, Michelle Kirschner, Benno Schwarz, Attila Borsos, Roscoe Jones, David Wolber, Amanda Neely, Dharak Bhavsar, Felicia Chen, Justin duRivage, Justin Fishman, Konstantinos Flogaitis*, Mason Gauch, Erika Suh Holmberg, Zach Kosbie, Hayley Lawrence, Allison Lewis, Nikita Malevanny, Jacob McGee, Chris Mullen, Sarah Pongrace, Nick Rawlinson, Anna Searcey, Samantha Sewall, Alana Sheppard*, Dominic Solari, Elsie Stone, Audi Syarief, Alana Tinkler, Lauren Trujillo, Gerti Wilson, Claire Yi, and Zach Young.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these issues. For additional information about how we may assist you, please contact the Gibson Dunn lawyer with whom you usually work, the authors, or the following leaders and members of the firm's International Trade practice group:

United States
Ronald Kirk – Co-Chair, Dallas (+1 214.698.3295, rkirk@gibsondunn.com)
Adam M. Smith – Co-Chair, Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)

Stephenie Gosnell Handler – Washington, D.C. (+1 202.955.8510, shandler@gibsondunn.com)
Christopher T. Timura – Washington, D.C. (+1 202.887.3690, ctimura@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202.887.3786, dburns@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213.229.7269, nhanna@gibsondunn.com)
Courtney M. Brown – Washington, D.C. (+1 202.955.8685, cmbrown@gibsondunn.com)
Chris R. Mullen – Washington, D.C. (+1 202.955.8250, cmullen@gibsondunn.com)
Sarah L. Pongrace – New York (+1 212.351.3972, spongrace@gibsondunn.com)
Anna Searcey – Washington, D.C. (+1 202.887.3655, asearcey@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)
Claire Yi – New York (+1 212.351.2603, cyi@gibsondunn.com)
Shuo (Josh) Zhang – Washington, D.C. (+1 202.955.8270, szhang@gibsondunn.com)

Asia
Kelly Austin – Hong Kong/Denver (+1 303.298.5980, kaustin@gibsondunn.com)
David A. Wolber – Hong Kong (+852 2214 3764, dwolber@gibsondunn.com)
Fang Xue – Beijing (+86 10 6502 8687, fxue@gibsondunn.com)
Qi Yue – Beijing (+86 10 6502 8534, qyue@gibsondunn.com)
Dharak Bhavsar – Hong Kong (+852 2214 3755, dbhavsar@gibsondunn.com)
Felicia Chen – Hong Kong (+852 2214 3728, fchen@gibsondunn.com)
Arnold Pun – Hong Kong (+852 2214 3838, apun@gibsondunn.com)

Europe
Attila Borsos – Brussels (+32 2 554 72 10, aborsos@gibsondunn.com)
Susy Bullock – London (+44 20 7071 4283, sbullock@gibsondunn.com)
Patrick Doris – London (+44 207 071 4276, pdoris@gibsondunn.com)
Sacha Harber-Kelly – London (+44 20 7071 4205, sharber-kelly@gibsondunn.com)
Michelle M. Kirschner – London (+44 20 7071 4212, mkirschner@gibsondunn.com)
Penny Madden KC – London (+44 20 7071 4226, pmadden@gibsondunn.com)
Irene Polieri – London (+44 20 7071 4199, ipolieri@gibsondunn.com)
Benno Schwarz – Munich (+49 89 189 33 110, bschwarz@gibsondunn.com)
Nikita Malevanny – Munich (+49 89 189 33 160, nmalevanny@gibsondunn.com)

**Konstantinos Flogaitis, a trainee solicitor in the London office, is not admitted to practice law.*

**Alana Sheppard, an associate in the New York office, is practicing under supervision of members of the New York bar.*

Related Capabilities

International Trade Advisory and Enforcement