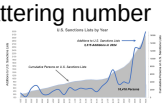
GIBSON DUNN

International Trade 2024 Year-End Update

Client Alert | February 6, 2025

The four years of the Biden administration were marked by the most aggressive and far-reaching use of international trade tools of any U.S. administration in history. Its final acts—some just days before the new administration took power—were among the most impactful of these measures. While there remains uncertainty about the Trump administration's trade policy, early indications are that the Trump team will wield these tools in an even more aggressive manner focused on an ever-larger set of policy goals—with unknown effects, both at home and abroad. Throughout 2024, the United States, the European Union, and the United Kingdom continued their fast-paced adoption and usage of the entire suite of international trade tools to exert pressure on Moscow, Beijing, and other targets. As but one indicator of his preference for the use of these tools, President Biden during his tenure imposed sanctions at a faster rate than any of his predecessors by adding thousands of names per year to restricted party lists maintained by the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"). That upswing accelerated in 2024 as the United States added a record-shattering number of, predominantly Russian, individuals and entities to OFAC sanctions lists:



Sanctions designations, however, tell only a small part of the story. Policymakers in Washington, London, and other capitals this past year also unveiled groundbreaking export controls, and focused on novel outbound investment regimes, in a bid to slow China's advances in certain critical technologies like semiconductors and artificial intelligence ("AI"). Following a wave of turnover in the White House, Downing Street, the EU institutions, and in other halls of power, the world's major economies appear poised to continue their heavy reliance on trade controls—though the mix of tools and targets could radically shift. Under President Trump, the United States appears set to favor aggressive threats and uses of tariffs (over other tools in the international trade arsenal), and, as we have already seen, may wield trade restrictive measures against both strategic competitors and core partners like Canada, Mexico, and the European Union. Other jurisdictions in Europe, Asia, and the Americas are likely to deploy those same tools, either in retaliation against U.S. measures or in pursuit of their own strategic interests. After several years of closely coordinated measures in support of common objectives such as impeding Russia's war in Ukraine, we anticipate a reshaped international trade landscape marked by friction among traditional allies and heightened uncertainty for the business community. **TABLE OF CONTENTS**

I. U.S. Sanctions

A. Russia B. Iran C. Syria D. Venezuela E. Cuba F. Crypto/Virtual Currencies G. OFAC Enforcement Trends

II. U.S. Export Controls

A. China B. Russia and Belarus C. Multilateral Controls D. End-Use and End-User Controls E. Compliance Expectations F. Voluntary Self-Disclosures G. BIS Enforcement Trends

III. U.S. Foreign Investment Restrictions

A. Inbound Investment B. Outbound Investment

IV. U.S. Import Restrictions

Related People

Scott R. Toussaint

Irene Polieri

Adam M. Smith

Stephenie Gosnell Handler

Christopher T. Timura

Ronald Kirk

Donald Harrison

Benno Schwarz

Michelle M. Kirschner

Attila Borsos

Samantha Sewall

Claire Shepherd

Alana Tinkler

Tina Asgharian

Karsten Ball

Dharak Bhavsar

Sarah Burns

Alexa A. Bussmann

Martin Coombes

Justin duRivage

Hui Fang

Anna Helmer

Erika Suh Holmberg

Vanessa Ludwig

Nikita Malevanny

Jayee Malwankar

Chris R. Mullen

Sarah L. Pongrace

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

A. Uyghur Forced Labor Prevention Act B. Tariffs

V. European Union

A. Sanctions B. Export Controls C. Foreign Investment Restrictions

VI. United Kingdom

A. Sanctions B. Export Controls C. Foreign Investment Restrictions

Anna Searcey

Audi K. Syarief

Roxana Akbari

I. U.S. Sanctions

A. Russia

Following the Kremlin's full-scale invasion of Ukraine in early 2022, the United States, in close coordination with its allies and partners, unleashed a historic barrage of trade restrictions on Russia. As the war in Ukraine stretched into a third year, the Biden administration in 2024 continued its shift from rapidly introducing new and often novel trade controls to incrementally expanding existing measures such as blocking sanctions, services prohibitions, import bans, and secondary sanctions. Such seemingly disparate measures were each calculated to deny Russia the capital and materiel needed to wage war in Ukraine. Notably, President Biden during his final months in the White House sharply increased sanctions on Russia's financial and energy sectors, including blacklisting major Russian banks and oil companies. Those actions, which aimed to restrict Moscow's access to the international financial system and limit its chief source of hard currency, also potentially increase his successor's leverage at the negotiating table. After his campaign trail vow to end the war in Ukraine on his first day in office failed to materialize, President Trump now at least appears poised to potentially further escalate sanctions and other trade measures in a bid to pressure the Kremlin (and Kyiv) into seeking a negotiated resolution to the conflict. Depending upon how events unfold, such U.S. measures could potentially include hiking tariffs on imported Russian goods, targeting additional oil producers, and wielding secondary sanctions against foreign banks that continue to engage with Russia. It is also likely that the Trump administration will seek to bring other, seemingly unrelated, issues—such as securing U.S. access to critical minerals—into any deal.

1. Blocking Sanctions

Since February 2022, the United States, in an unprecedented burst of activity, has added thousands of new Russia-related individuals and entities to OFAC sanctions lists. That trend intensified during the final year of the Biden administration as the United States, on eight separate occasions, added 100 or more new Russia-related targets to OFAC's Specially Designated Nationals and Blocked Persons ("SDN") List—an extraordinary pace considering that around 13,000 parties had been added to the SDN List over the preceding twenty years combined. 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 SDN List therefore functions as the United States' principal sanctions-related restricted party list. Moreover, the effects of blocking sanctions often reach beyond the parties identified by name on the list. By operation of OFAC's Fifty Percent Rule, restrictions generally also extend to entities owned 50 percent or more in the aggregate by one or more blocked persons, whether or not the entity itself has been explicitly identified. During 2024 and continuing into early 2025, the United States repeatedly used its targeting authorities to block Russian business elites, as well as substantial enterprises operating in sectors such as banking, energy, and technology seen

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

as critical to financing and sustaining the Kremlin's war effort. Notable designations included:

- Oligarchs such as the chief executive officers of several major Russian oil companies;
- Financial institutions, including ***Gazprombank***, the ***Moscow Exchange***, Russia's ***National Settlement Depository***, and dozens of Russian securities registrars, further severing Russia's access to the international financial system;
- Energy firms such as ***Gazprom Neft*** and ***Surgutneftegas***, which were targeted to limit Russia's current energy revenues and future extractive capabilities;
- Shipping companies such as ***Sovcomflot*** and ***Rosneftflot***, to impede the transport of Russian-origin petroleum and petroleum products to overseas buyers;
- Military-industrial firms, including hundreds of companies operating in the technology, defense and related materiel, construction, aerospace, and manufacturing sectors of Russia's economy; 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 hundreds of parties located in major transshipment hubs such as Turkey, the United Arab Emirates, and the People's Republic of China ("PRC").

Substantially all of the parties described above were designated pursuant to Executive Order ("E.O.") 14024, as amended, a measure that President Biden signed at the outset of his term that 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. Throughout President Biden's tenure, OFAC relied almost exclusively on E.O. 14024 to target new Russia-related parties. However, during its final days in office, the administration broadened its use of blocking sanctions in two novel respects. The Biden administration in January 2025 added a further sanctions basis to over 100 Russian parties by re-designating key targets—including major oil companies, shippers, manufacturers, and banks—pursuant to an earlier Obama-era authority, Executive Order 13662. Sanctions on those entities under E.O. 14024 remained in place. Although imposing blocking sanctions under additional authorities did not result in those targets becoming subject to further restrictions, the use of E.O. 13662 raises the procedural bar for easing sanctions on such persons by triggering a unique congressional review mechanism in the Countering America's Adversaries Through Sanctions Act ("CAATSA"). Consequently, the Trump administration is now obliged to submit a detailed report to Congress and, absent congressional action, wait a specified number of days before lifting sanctions on any parties that have been designated under E.O. 13662—which appears calculated to delay, and increase the domestic political costs of, a possible future effort by President Trump to relax sanctions on Russia. Concurrent with that announcement, the Biden administration further expanded the potential bases upon which parties can become designated for engaging with Russia. Building upon the various sectors that had been identified in prior years, the Biden administration in January 2025 authorized the imposition of blocking sanctions on parties that operate in Russia's energy sector, which OFAC broadly defines to include upstream, midstream, and downstream activities related to oil, natural gas, and other products capable of producing or transporting energy. Crucially, OFAC has indicated that parties operating in targeted 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 years of treading lightly around Russian oil and gas producers to avoid roiling global markets, the Biden administration in its final weeks appears to have been emboldened by more stable energy supplies to sharply restrict dealings involving Russia's extractive industries. Notwithstanding the considerable policy differences between the two administrations, President Trump, at least in the near term, appears likely to maintain and potentially expand U.S. sanctions on Russian energy to maximize U.S. leverage in future

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

negotiations with Moscow.

2. Services Prohibitions

Since the opening months of the war in Ukraine, the United States has supplemented its use of blocking sanctions against targeted individuals and entities by banning U.S. persons from exporting to Russia 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 two years of the war barred U.S. exports to Russia of certain categories of services that, if misused, could enable sanctions evasion , bolster the Russian military, and/or contribute to Russian energy revenues. In April 2024, the United States expanded upon those earlier prohibitions by barring the exportation to Russia of certain services related to the acquisition of Russian-origin aluminum, copper, or nickel to limit the trading of Russian metals on global exchanges. In June 2024, OFAC, in close coordination with the U.S. Department of Commerce's Bureau of Industry and Security ("BIS"), restricted exports to Russia of information technology ("IT") consultancy and design services, as well as IT support services and cloud-based services for certain types of widely used business software, to prevent U.S. technical expertise and Software as a Service ("SaaS") offerings from being leveraged by Russia's military-industrial base. In conjunction with the imposition of blocking sanctions against several major Russian oil companies (discussed above), the Biden administration in January 2025 further limited U.S. person activities by, effective February 27, 2025, prohibiting the exportation to Russia of petroleum services, which OFAC defines in expansive terms to include "services related to the exploration, drilling, well completion, production, refining, processing, storage, maintenance, transportation, purchase, acquisition, testing, inspection, transfer, sale, trade, distribution, or marketing of petroleum, including crude oil and petroleum products." As such, absent an exclusion—such as for services related to the maritime transport of Russian crude oil or petroleum products purchased at or below a specified price cap—or authorization from OFAC in the form of a license, U.S. persons starting in late February potentially risk U.S. sanctions exposure for providing services that enable Russia to exploit its hydrocarbon resources.

3. Import Prohibitions

Consistent with a whole-of-government approach to limiting Russian revenue, the United States during 2024 continued to expand prohibitions on the importation 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. In prior years, the Biden administration used this particular policy tool to bar imports into the United States of certain energy products of Russian Federation origin, fish, seafood, alcoholic beverages, non-industrial diamonds, and gold. As with other Russia-related sanctions authorities, the Secretary of the Treasury has broad discretion under Executive Order 14068, as amended , to, at some later date, extend the U.S. import ban to additional Russian-origin goods. The Biden administration during the past year wielded that authority to prohibit the importation into the United States of additional Russian commodities, including additional categories of diamonds and diamond jewelry, as well as aluminum, copper, and nickel. Highlighting the degree of bipartisan support for limiting Russia's access to the U.S. market, the U.S. Congress in May 2024 enacted legislation barring the importation into the United States of Russian-origin low-enriched uranium. Although most other imports of Russian-origin items remain permissible under U.S. law, bilateral trade in goods between the United States and Russia plunged to a 30-year low in 2024 and appears unlikely to rebound absent a sea change in relations between Washington and Moscow. As it has been since the start of the 2022 invasion, the implications of trade restrictions will be felt much more by countries in Europe and Asia that have far more robust trading relationships

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

with Moscow.

4. Secondary Sanctions

As part of a broader effort to limit sanctions and export control evasion, the United States in late 2023 authorized secondary sanctions on foreign financial institutions that, knowingly or unknowingly, facilitate significant transactions involving Russia's military-industrial base. As we observe in a prior client alert, these 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 their customers' trade in certain enumerated goods, and do so under a standard of strict liability (i.e., without requiring any intent or even having knowledge of the activity). This is a meaningful departure from historical practice. Under certain U.S. sanctions programs—namely, those targeting Iran, North Korea, Russia, Syria, Hong Kong, and terrorism—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 potentially relatively innocuous (e.g., blocking their 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—essentially adding them to the SDN List). 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. The Biden administration in December 2023 issued Executive Order 14114 authorizing OFAC to impose secondary sanctions on foreign financial institutions that are deemed to have:

- Conducted or facilitated a significant transaction involving a person that has been blocked for operating in certain sectors of Russia's economy (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 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. In June 2024, in recognition of Russia's transition to a wartime economy, the United States broadened the reach of U.S. secondary sanctions by publishing updated guidance that expands OFAC's interpretation of "Russia's military-industrial base" to include not only persons that have been blocked for operating in certain sectors of Russia's economy—formerly, the technology, defense and related materiel, construction, aerospace, or manufacturing sectors—but *all* persons blocked pursuant to Executive Order 14024. As a practical matter, that shift both simplifies compliance for foreign financial institutions by eliminating the need to assess whether a transaction party

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

is among a subset of Russian SDNs that can give rise to secondary sanctions exposure, and enhances the deterrent effect of U.S. sanctions by expanding the universe of Russia-related transactions that can place a foreign bank at risk of losing access to the U.S. financial system. Notably, the Biden administration invoked that secondary sanctions authority for the first time in January 2025 by imposing blocking sanctions on a Kyrgyzstan-based bank for allegedly processing payments on behalf of a blocked Russian bank with close ties to Russia's defense industry. Although the use of U.S. secondary sanctions against banks that continue to engage with Russia is so far limited and isolated, to the extent President Trump is inclined to escalate pressure on Moscow, that designation could offer the new administration a model for targeting progressively larger foreign financial institutions that continue to process Russia-related trade.

5. Prospects for Further Sanctions on Russia

As President Trump looks to deliver on his oft-repeated campaign pledge to end the war in Ukraine, the United States could soon further tighten trade restrictions in an attempt to push Moscow to the negotiating table. Options available to the Trump administration under such an approach include increasing tariffs on the limited volume of Russian goods still imported into the United States or, more consequentially, targeting Russia's crucial financial and energy sectors by imposing blocking sanctions on all remaining Russia-based banks and oil majors ***Rosneft*** and ***Lukoil***. It is also conceivable that the new administration could, in a bid to constrict Moscow's oil revenues, threaten to impose secondary sanctions on foreign financial institutions (including especially in China and India) that continue to process payments involving Russian petroleum and petroleum products. Conversely, if eventual talks among Washington, Moscow, and Kyiv show signs of progress, it would not be surprising if the White House just as quickly eases restrictions on dealings involving Russia. With the exception of the E.O. 13662 re-designations noted above, nearly all of the Biden-era measures targeting Russia (which were implemented via Executive Order) can be—as President Trump demonstrated in his first days in office—rescinded with the stroke of a pen. For example, President Trump could narrow or revoke existing measures such as the prohibition on "new investment" in the Russian Federation set forth in E.O. 14071 by issuing new or amended Executive Orders, or by issuing permissive general licenses. Any such relaxation of U.S. sanctions could, however, result in a split between the United States and its European allies and partners, who to date have shown little appetite for easing their own considerable restrictions on Russia. President Trump's return to power also casts into doubt an unprecedented effort to leverage Russia's sovereign assets to fund Ukraine's defense and reconstruction. As the cost of the war continued to mount, the United States and its partners during 2024 explored a range of options to deploy the nearly $300 billion in Russian central bank reserves, principally held in Europe, that the allies immobilized in the opening weeks of the conflict. At a June 2024 summit, the Group of Seven ("G7") ultimately agreed on a novel mechanism whereby the allies would extend $50 billion in loans to Ukraine, to be paid down over time by the interest that is continuing to accrue on the Kremlin's assets held abroad. That U.S.-led initiative—dubbed the Extraordinary Revenue Acceleration Loan program—resulted in the United States disbursing a $20 billion loan to Kyiv in December 2024, with a separate €3 billion loan from the European Commission following in January 2025. While stopping short, at least so far, of seizing Russian state property, the loan program nevertheless has potentially fundamental consequences for global finance, which heretofore held a nearly unshakable belief in the immunity of sovereign assets—especially of major states.

B. Iran

Iran suffered a series of strategic setbacks in 2024, including a deepening economic crisis, multiple rounds of Israeli airstrikes, the decimation of Hamas and Hezbollah's senior leadership, and the collapse of the Assad regime in Syria. Following President Trump's return to the White House, Tehran could soon be forced to decide whether to pursue negotiations aimed at securing sanctions relief, or race for a nuclear weapon to restore the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Islamic Republic's battered deterrence. As these developments unfolded, the Biden administration during 2024 continued to aggressively use its sanctions authorities to add individuals and entities complicit in Iran's destabilizing activities to the SDN List. Frequent targets of Iran-related designations included Iranian government officials, entities involved in unmanned aerial vehicle ("UAV") and ballistic missile procurement, and entities and vessels involved in the Iranian petroleum and petrochemicals trade. The pace of Iran sanctions designations could further increase under President Trump as part of the resumption of his first term's "maximum pressure" economic campaign, which he announced on February 4, 2025. That effort aims to deny Tehran the resources needed to fund its terrorist proxies. An accompanying national security memorandum previewed the Trump administration's likely targeting of third-country shipping companies, insurers, and port operators that enable Iranian oil exports. If need be, the pressure campaign could potentially invoke legislation enacted in April 2024, including the Stop Harboring Iranian Petroleum Act and the Iran-China Energy Sanctions Act of 2023, that authorizes the President to impose sanctions on non-U.S. persons, including especially in China, that are involved in bringing Iranian oil to market.

C. Syria

U.S. sanctions on Syria were largely quiet for much of the past year, until the sudden December 8, 2024 ouster of Syria's longtime ruler Bashar al-Assad following a brutal, decade-long civil war. Despite the Assad regime's collapse, Syria—alongside a small handful of other jurisdictions, presently including Cuba, Iran, North Korea, and certain Russian-occupied regions of Ukraine—remains subject to comprehensive U.S. sanctions, as a result of which U.S. persons are generally prohibited from engaging in transactions involving that country. Further complicating efforts to stabilize Syria and rebuild its shattered economy, the rebel group that in December 2024 became the country's *de facto* governing authority, Hayat Tahrir al-Sham ("HTS"), and its leader Ahmed Hussein al-Sharaa (formerly known by the *nom de guerre* Abu Mohammed al-Jawlani), each remain subject to U.S. blocking sanctions for their historical ties to the Islamic State and al Qaeda. In January 2025, the United States announced a narrow and time-limited suspension of certain U.S. restrictions to "ensure that sanctions do not impede essential services and continuity of governance functions across Syria, including the provision of electricity, energy, water, and sanitation." In particular, OFAC issued a general license that authorizes U.S. persons, until July 7, 2025, to engage in certain transactions involving: (1) Syria's post-Assad governing institutions; (2) the sale, supply, storage, or donation of energy, including petroleum, petroleum products, natural gas, and electricity, to or within Syria; and (3) processing the transfer of noncommercial, personal remittances to Syria, including through the Central Bank of Syria. The authorizations set forth in that license exclude, among other things, any transactions involving military or intelligence entities or new investment in Syria by U.S. persons. Notably, the license authorizes financial transfers to blocked persons such as HTS for specified purposes such as effecting the payment to governing institutions in Syria of taxes, fees, or import duties—suggesting a U.S. policy interest in enabling the continuing functioning of the Syrian state, notwithstanding HTS and al-Sharaa's status as designated terrorists. Both the Biden and Trump administrations appear to have otherwise adopted a wait-and-see approach to Syria sanctions relief, with the further easing of U.S. restrictions likely contingent upon HTS demonstrating tangible progress toward forming an inclusive transitional government, protecting the rights of ethnic and religious minorities, pledging not to serve as a conduit for the export of Iranian destabilization, and responsibly disposing of Syria's chemical weapons. In light of President Trump's aggressive use of U.S. counterterrorism sanctions authorities during his first week in office—including to target drug cartels and the Yemen-based Houthis—the United States seems unlikely to lift blocking sanctions on HTS and its leader Ahmed Hussein al-Sharaa, at least in the near future.

D. Venezuela

The United States in early 2024 withdrew two short-lived forms of sanctions relief after

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Venezuela's President Nicolás Maduro failed to uphold his commitments to take concrete steps toward holding free and fair elections. As we describe in a prior client alert, the Biden administration in October 2023 announced a significant relaxation of U.S. sanctions on Venezuela in an attempt to incentivize the Maduro regime to take concrete 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 in January 2024 quickly revoked a general license that had authorized U.S. nexus transactions involving Venezuela's state-owned gold mining company—and warned that, absent a change in behavior by the Maduro regime, a separate general license authorizing most dealings involving the country's oil or gas sector would meet a similar fate. A further tightening of U.S. sanctions followed in April 2024 when the Biden administration made good on that threat and allowed Venezuela General License 44 to expire—with the result that, unless separately authorized by OFAC, U.S. persons are again generally prohibited from engaging in transactions involving the state-owned oil giant ***Petróleos de Venezuela, S.A.*** ("PdVSA"). Following a July 2024 presidential contest marred by widespread irregularities, the United States recognized opposition candidate Edmundo González as the country's president-elect—to little effect, as Maduro clung to power and was sworn in for a third term in January 2025. While democratization efforts have historically been the guide by which prior administrations have assessed the need for sanctions on Caracas, under the new Trump administration it appears that willingness to stem illegal immigration may serve as a favored guide in this regard. Indeed, we assess that if there is a Washington-Caracas deal to stem the flow of Venezuelan migrants northward, the United States under President Trump and Secretary of State Marco Rubio could opt to institute some easing of measures. January 2025 meetings between the Trump administration's envoy for special missions Richard Grenell and the Maduro government resulted in Venezuela's release of several U.S. prisoners, suggesting that a deal may be sought. However, in the absence of such a deal, we assess it as likely that we will see a further tightening of sanctions on the Maduro regime, including a potential narrowing or revocation of existing authorizations to engage with Venezuela's crucial oil sector or a resumption of President Trump's first-term practice of aggressively designating shipping companies and vessels that bring Venezuelan oil to market.

E. Cuba

During 2024, U.S. sanctions on Cuba continued their decades-long trend of swinging sharply back and forth, depending upon whether Republicans or Democrats control the White House. During his waning months in power, President Biden modestly eased restrictions on Havana, including by authorizing U.S. banks to process certain Cuba-related payments and de-listing Cuba as a State Sponsor of Terrorism. However, that relief was short-lived, as President Trump unwound many of those same measures within hours of returning to the Oval Office. Under the first Trump administration, the United States in 2019 prohibited U.S. banks from processing so?called "U?turn" payments. These transactions—which involve Cuban interests and originate from, and terminate, outside of the United States—enable Cuban entities doing business with non?U.S. firms to access U.S. correspondent and intermediary banks and therefore to participate in U.S. Dollar?denominated global trade. In May 2024, as part of a package of incremental changes to the Cuba regulations, the Biden administration issued a general license authorizing U.S. banks to again process such Cuba-related payments, provided that neither the originator nor the beneficiary, nor their respective banking institution, is a person subject to U.S. jurisdiction. From a policy perspective, the Biden administration appears to have been aiming to increase independent Cuban entrepreneurs' access to the international financial system. In a more sweeping—though, it turned out, temporary—reversal of Trump-era policy, President Biden on January 14, 2025 announced a Vatican-brokered agreement to secure the release of hundreds of Cuban political prisoners. In exchange, the United States rescinded Cuba's designation as a State Sponsor of Terrorism, suspended a private right of action that had enabled lawsuits in U.S. courts against individuals and companies accused of "trafficking" in property confiscated by the Cuban government, and revoked a memorandum that

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

underpins the U.S. ban on direct financial transactions involving certain entities identified on the State Department's Cuba Restricted List. Reflecting the ongoing tug-of-war over Cuba policy, President Trump less than a week later rescinded each of those measures on his first day in office. As such, U.S. sanctions on Cuba are now, with modest exceptions, substantially similar to the restrictions that were in place when President Trump left office in 2021. To the extent President Trump and Secretary Rubio are inclined to further increase sanctions on Cuba, it is possible that the new administration could in coming months eliminate the authorization for "U-turn" payments, as well.

F. Crypto/Virtual Currencies

OFAC throughout the past several years has closely focused on illicit finance in the virtual currency sector, including through a mix of new sanctions designations and aggressive enforcement actions. However, a recent court decision finding that OFAC lacks authority to impose sanctions on immutable smart contracts, coupled with the Trump administration's promises of lighter-touch regulation of the industry, could portend a shift in OFAC's priorities away from digital assets and toward other sectors of the economy such as traditional finance. In August and November 2022, OFAC imposed blocking sanctions on the virtual currency mixer ***Tornado Cash***. Virtual currency mixers, as the name suggests, operate by mixing together funds deposited by many users before transmitting the funds to their individual recipients, thereby obfuscating the parties to a transaction. That designation represented a novel use of U.S. sanctions as, unlike a centralized platform in which a single company processes virtual currency transactions, Tornado Cash's decentralized, smart contract model is essentially operated by self-executing code running on public blockchains without the need for human intervention. Tornado Cash users soon filed suit, arguing that there is no "person" or "property" for OFAC to sanction. In November 2024, the U.S. Court of Appeals for the Fifth Circuit, in a still-rare successful court challenge to a U.S. sanctions determination, held that OFAC exceeded its authority when it designated Tornado Cash's immutable smart contracts (i.e., unalterable, open-source, privacy-enabling software code) as blockable property. In particular, the Fifth Circuit in *Van Loon v. U.S. Department of the Treasury* reasoned that, to constitute "property," something must be "capable of being owned," which in turn requires that an owner be capable of exercising "dominion" over it. The Court concluded that immutable smart contracts are unownable and therefore not "property" because they cannot be altered nor can anyone be excluded from using them. The *Van Loon* decision is noteworthy as it adds to a growing body of jurisprudence (discussed further below) limiting the authority of administrative agencies and, absent intervention by Congress, could complicate OFAC's ability to restrict dealings involving digital assets going forward. We expect more challenges to OFAC actions in the wake of the U.S. Supreme Court's June 2024 decision in *Loper Bright Enterprises v. Raimondo* (discussed below), which eliminated the requirement that courts defer to agencies' reasonable interpretations of the statutes that they administer, and on which the *Van Loon* Court relied in reaching its conclusion. In contrast with the Biden administration's aggressive regulatory approach to the virtual currency sector, a second Trump administration seems likely to usher in a more permissive regulatory environment. Underscoring the White House's expected posture toward the virtual currency industry, President Trump shortly before taking office launched his own digital token and, once in the White House, quickly issued an Executive Order directing an overhaul of U.S. digital assets policy. Following several years of robust U.S. sanctions enforcement against virtual currency industry participants, it is possible that OFAC could in coming months recalibrate its enforcement approach to once again prioritize other sectors.

G. OFAC Enforcement Trends

1. Enforcement Actions and Compliance Lessons

During 2024, the combined amount of civil monetary penalties imposed by OFAC fell back in line with the agency's long-term average after hitting a record-shattering $1.5 billion the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

year prior. That decline was principally driven by the absence of any blockbuster, nine-figure settlements. Across 12 enforcement actions resulting in monetary penalties, OFAC in 2024 levied an aggregate of $48.8 million in fines—an amount roughly on par with 2022 ($42.6 million) and modestly higher than 2021 or 2020 (both around $20 million). The two largest resolutions this past year involved monetary penalties of $20 million and $14.5 million, both stemming from alleged violations of U.S. sanctions on Iran. While enforcement actions are often a trailing indicator of OFAC enforcement priorities (given that matters can take several years to resolve after a violation has been found), this trend nonetheless suggests that dealings involving the Islamic Republic are likely to remain an area of continued focus for U.S. authorities during the months ahead. We highlight below the most noteworthy compliance lessons from OFAC's 2024 enforcement actions, many of which are thematically consistent with prior years. Some of these takeaways were explicitly communicated by OFAC through the "compliance considerations" section included in the web notice for each of its enforcement actions:

- **Dealings in and around Iran can present heightened risks**: Half of OFAC's 12 cases announced during 2024 involved apparent Iran sanctions violations and highlight the importance (and expectation) of effective due diligence. OFAC, for example, suggested in a November 2024 settlement that companies' due diligence efforts should take into account that sanctioned Iranian parties might not necessarily appear by name on the SDN List and may often be based in nearby jurisdictions such as the United Arab Emirates. The Trump administration's February 2025 resumption of the Iran "maximum pressure" campaign explicitly ordered the expansion of enforcement efforts.
- **Non-U.S. companies should ensure that their activities do not "cause" U.S. persons to violate U.S. sanctions restrictions**: Five non-U.S. companies were penalized this past year for "causing" a U.S. person (such as a U.S. correspondent bank) to violate their own sanctions compliance obligations—a common fact pattern in recent years. OFAC has long maintained that non-U.S. companies are on notice of this obligation when they avail themselves of U.S. customers, goods, technology, or services. Non-U.S. companies should therefore be mindful that, even in cases in which an undertaking on its face has no readily discernable U.S. touchpoint, they must comply with U.S. sanctions when engaging in a transaction that involves even a fleeting U.S. touchpoint such as clearing a U.S. Dollar-denominated payment through a U.S. financial institution.
- **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 implementing and maintaining proper compliance controls, such as policies for U.S. person directors, officers, and employees to recuse themselves from prohibited activities and whistleblower mechanisms to identify prohibited conduct.
- **Companies should remain vigilant for efforts by persons in Russia and Russian-occupied regions of Ukraine to evade sanctions**: Two of OFAC's 12 published cases this past year alleged violations of its Ukraine- and Russia-related sanctions. Although that figure represents a much lower share of OFAC's cases than during the prior year, a lower enforcement rate does not necessarily indicate that OFAC deprioritized Russia-related sanctions. Rather, given the volume and complexity of new restrictions on Russia announced since February 2022—and the amount of time that is often required for OFAC to conduct a fulsome investigation—it is highly likely that further Russia-related enforcement actions could be announced in coming months.

During January 2025, OFAC announced two further settlements resulting in civil monetary penalties, offering an early indication that OFAC is likely to continue aggressively enforcing U.S. sanctions prohibitions throughout the coming year.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

2. Statute of Limitations and Supreme Court Cases

Although the Executive branch is responsible for enforcing U.S. sanctions, key developments out of the U.S. Congress and the Supreme Court in 2024, including an expanded statute of limitations for sanctions violations and a growing body of case law limiting judicial deference to administrative agencies, could further reshape both OFAC's enforcement of violations and its designation of parties to sanctions lists going forward. On April 24, 2024, President Biden signed into law the 21st Century Peace Through Strength Act, which extends the longstanding statute of limitations for civil and criminal violations of U.S. sanctions from five to ten years. That provision, which Congress quietly inserted into a foreign aid package, appears likely to increase the size of OFAC civil monetary penalties going forward by enabling the agency to reach a broader universe of violative transactions. Notably, OFAC in July 2024 published guidance affirming that the law did *not* revive civil or criminal sanctions violations that were time barred on the date that the new statute of limitations was enacted into law (i.e., April 24, 2024). As such, absent extenuating circumstances (such as a prior tolling agreement with OFAC), sanctions violations that occurred on or before April 24, 2019 are generally time barred and the new statute of limitations is, as a practical matter, being phased in over the next five years. Nevertheless, the new ten-year statute of limitations quickly shifted the landscape for compliance-minded companies. Starting on March 12, 2025, parties that engage in transactions that implicate OFAC's prohibitions will be required to retain relevant records for a period of ten years. The new statute of limitations also alters expectations concerning an appropriate "lookback" period for sanctions-related investigations, mergers and acquisitions due diligence, and representations and warranties in transactional agreements. In light of the potential for increased civil monetary penalties that sweep in twice as much conduct, the expanded statute of limitations could also affect parties' calculus regarding whether, and under what circumstances, to voluntarily self-disclose to OFAC apparent violations of the agency's regulations. Meanwhile, two U.S. Supreme Court decisions announced in June 2024—*Loper Bright Enterprises v. Raimondo* and *Securities and Exchange Commission ("SEC") v. Jarkesy*—threaten to complicate OFAC's longstanding practices by potentially forcing the agency to litigate more frequently and with a lower degree of judicial deference. As described more fully in a pair of prior client alerts, the Court in *Loper Bright* overruled *Chevron v. Natural Resources Defense Council* under which U.S. courts were formerly required to defer to agencies' reasonable interpretation of ambiguous statutory terms. In place of *Chevron*, courts now must independently interpret statutes and are no longer obligated to defer to agencies, though they may afford agencies' views a measure of "respect" to the extent those views are persuasive. In a separate opinion handed down that same week, the Court in *Jarkesy* held that the U.S. Constitution requires the SEC to sue in federal court, not an in-house administrative court, when seeking civil monetary penalties on a ground such as fraud that resembles a traditional action at common law. As lower courts continue to wrestle with the implications of *Loper Bright* and *Jarkesy*, those two cases taken together have the potential to unsettle U.S. sanctions and export controls by encouraging prospective litigants to challenge agency action, channeling more such disputes into U.S. federal court, and resetting the balance of power between challengers and federal agencies such as OFAC and BIS. Accordingly, following a sustained two-decade rise in the use of sanctions and export controls as primary instruments of U.S. foreign policy, OFAC and BIS could soon be forced to weigh whether, in the face of potential legal challenges, they are prepared to continue pushing the limits of their authorities by levying substantial monetary penalties out of court. **II. U.S. Export Controls** U.S. export controls during 2024 continued their rise as indispensable and central tools to further U.S. national security and foreign policy objectives. A key focus of U.S. efforts involved developing new ways to restrict access to certain advanced technologies by perceived geopolitical competitors like China, while allowing for the continued exchange of these technologies among countries that adopt restrictions that parallel U.S. controls. Rules issued by the U.S. Department of Commerce's Bureau of Industry and Security have always been technical and fact-dependent; indeed, the rules have often required significant scientific knowledge to understand and implement them appropriately. While BIS rules have steadily become more complex, the regulations

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

announced in 2024 accelerated this trend, underlining the sophisticated nature of export controls while emphasizing the need for exporters to have a highly nuanced and technically informed understanding of exactly what they are, directly or indirectly, exporting, reexporting, or transferring, and to whom. Developments in 2024 also highlighted the increasing risks for violations of these rules, with the U.S. Department of Justice ("DOJ") and BIS both articulating new rules and expectations in order to avoid serious penalties. Moreover, for the first time, the necessity of understanding these rules has been expanded from exporters themselves to financial intermediaries such as banks. As discussed below, BIS published an unprecedented set of expectations for financial institutions regarding their obligations to ensure compliance with export controls. This was a meaningful departure from past practice—which had placed the onus and risk for compliance chiefly on exporters. Financial institutions have started to develop protocols in this regard, but industry "best practices" remain a work in progress. Technology is developing so rapidly that export control regulations are unable to keep pace. As such, we fully expect new regulations to be frequently issued, further refining and likely expanding areas of control.

A. China

Throughout 2024, BIS continued to focus on tightening controls on the People's Republic of China and other countries posing diversion risks with respect to semiconductor manufacturing equipment ("SME"), advanced computing items, and quantum computing technology. These efforts led to a flurry of new rulemaking activity over the past year and created many new compliance obligations across industries. While the Trump administration's export control priorities remain opaque, the compliance complexities associated with these efforts are unlikely to abate.

1. Advanced Computing Items, Semiconductor Manufacturing Equipment, and Supercomputers

Senior U.S. officials, including then-National Security Advisor Jake Sullivan, often described controlling semiconductors as among the Biden administration's top foreign policy priorities and announced their intention to prevent China from acquiring the most sophisticated chips to slow Beijing's military modernization. Consistent with that approach, BIS in April 2024 released an interim final rule imposing additional restrictions on SME, advanced computing items, and items supporting supercomputing end uses exported to the PRC and certain "Country Group D" destinations. This new rule also provided clarity to previous semiconductor and supercomputing-related rules issued in October 2022 and October 2023, which we describe in more detail in two prior client alerts. Interim final rules relating to national security generally become effective immediately on the date that they are released for public inspection in the U.S. Federal Register. The public is invited to submit comments even while implementing the new rule, and these comments will be considered by the agency in drafting a final rule that will supersede the interim final rule once released. In recent years, both the U.S. Department of Commerce and the U.S. Department of the Treasury have used the rulemaking process to engage with various stakeholders in crafting rules on a variety of topics, often due to the breadth of proposed rules, even though such procedural steps are not required for most rules implicating national security concerns. BIS's April 2024 interim final rule amends the U.S. Export Administration Regulations ("EAR")—which are the principal U.S. regulations governing exports of goods, software, and technology that have both military and civilian uses (commonly known as "dual-use" items)—in several notable respects, including:

- The bifurcation of License Exception Notified Advanced Computing ("NAC") into two new license exceptions.
- A license exception authorizes otherwise licensable exports to specified end users, end uses, or destinations. In general, license exceptions are open to any non-

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

restricted party, and they can be used without seeking specific approval from the U.S. Government, provided that any applicability and recordkeeping requirements are met.

- In this case, License Exception NAC was split into:
    - A revised License Exception NAC authorizing exports and reexports of specified items to (1) Country Group D:5 destinations—which includes destinations subject to a U.S. arms embargo (i.e., Afghanistan, Belarus, Burma/Myanmar, Cambodia, Central African Republic, China (including Hong Kong), Cuba, Democratic Republic of the Congo, Eritrea, Haiti, Iran, Iraq, Lebanon, Libya, Nicaragua, North Korea, Russia, Somalia, South Sudan, Sudan, Syria, Venezuela, and Zimbabwe)—plus Macau, and (2) entities headquartered in, or with an ultimate parent headquartered in, a Country Group D:5 destination or Macau, subject to a pre-export notification requirement and revised procedures. The rule also clarifies that notification requirements for covered integrated circuits apply to computers and other products incorporating such items.
    - A new License Exception Advanced Computing Authorization ("ACA") authorizing (1) exports, reexports, and transfers (in-country) of specified items worldwide (except to or within Country Group D:5 destinations, Macau, or an entity headquartered in, or whose ultimate parent is headquartered in, a Country Group D:5 destination or Macau, wherever located), and (2) transfers (in-country) within a Country Group D:5 destination or Macau. Exports, reexports, and transfers under License Exception ACA are not subject to the BIS notification requirement, partly in an attempt to minimize the compliance burden on industry.
- Clarification that all exports, reexports, or transfers made pursuant to License Exceptions NAC or ACA require a written purchase order unless specifically exempted.
- Clarification that License Exceptions NAC and ACA are in addition to, not in lieu of, the requirements of License Exception Encryption Commodities, Software, and Technology ("ENC") and that License Exceptions NAC and ACA cannot be used if additional end-user or end-use restrictions (under 15 C.F.R. Part 744) or embargo restrictions (under 15 C.F.R. Part 746) apply.
- Revisions to BIS's license review policies specific to covered items, destinations, and end users.
- Due to a previous inadvertent omission, addition of extreme ultraviolet lithography masks to controls targeting the activities of U.S. persons.
- Revision of end-user controls to address support for indigenous "development" and "production" of front-end integrated circuit "production" equipment in Macau and destinations in Country Group D:5 countries, as well as confirmation that parts and components exported for ultimate incorporation into indigenous SME in the PRC also require a BIS license for the initial export.
- Revisions to several Export Control Classification Numbers ("ECCNs") to correct inadvertent errors, provide clarifications, and to control new items such as monolithic microwave integrated circuit amplifiers, missile-related items, pulse discharge capacitors, and superconducting solenoidal electromagnets, among others.

Collectively, these changes represent significant alterations to the earlier October 2022 and October 2023 controls and underscore the need to remain vigilant to frequent changes in the controls applicable to SME, advanced computing items, and quantum computing technology.

2. Quantum Computing

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

In September 2024, BIS released an interim final rule imposing additional controls, in conjunction with partner countries, on quantum computing (an emerging field within computer science that uses insights from physics to solve certain problems far faster than traditional computers) and other advanced technologies. This was a clear example of President Biden's preference for multilateral actions (discussed further below), and also recognized that without joint action the effectiveness of any export restriction will be far reduced. Specifically, the new rule made the following key changes to the EAR:

- Revision of several existing ECCNs and identification of a new subset of "900" series ECCNs (e.g., ECCN 3A**9**01), signifying controls harmonized with the implemented export controls of partner countries. Compared to items subject to multilateral regimes controls (e.g., the Wassenaar Arrangement), these "900" series items have worldwide license requirements and more limited license exception availability. Such items include, among other things, certain additive manufacturing equipment designed to produce metal or metal alloy components, technology for the development or production of coating systems, complimentary metal-oxide semiconductor circuits, parametric signal amplifiers, cryogenic cooling systems and components, gate all-around field-effect transistor ("GAAFET") technology, scanning electronic microscopes, cryogenic wafer probing equipment, various materials used to develop quantum items, software designed to extract Graphic Design System II or equivalent standard layout data, and quantum computers, as well as certain related equipment, software, and technology for such items.
- Imposition of deemed export and deemed reexport license requirements for certain quantum, integrated circuit, additive manufacturing, and aerospace items, a significant departure from similar controls previously imposed on certain SME and advanced computing items. However, BIS continues to include deemed export and deemed reexport license exclusions with respect to ECCNs 3D001, 3D002, and 3E001 for anisotropic dry plasma etch equipment and isotropic dry etch equipment, and there is a limited exclusion for certain software or technology released to persons whose most recent citizenship or permanent residency is not a country in Country Group D:1 or D:5. Deemed exports are exports that the U.S. Government "deems" to occur between the United States and a foreign person's home country when technology is shared with a foreign person physically located in the United States. Deemed reexports are exports that occur when technology is shared with a foreign person who has a nationality other than that of the foreign country where the release or transfer takes place. The list of software and technology eligible for this limited exclusion was amended in December 2024.
    - In light of personnel shortages in critical quantum-related fields, foreign person employees and contractors that already have access to covered software and technology as of September 6, 2024—particularly those in Country Group A:5 and A:6 destinations—are "grandfathered" in to allow continued access to this information. These shortages are so severe that even foreign persons who are existing employees or contractors and whose most recent country of citizenship or permanent residency is in Country Group D:1 or D:5 may continue to access sensitive GAAFET technology under the general license in the EAR's General Order No. 6. However, this is only the case if their employer conducts annual reporting. In some cases, personnel with experience in other kinds of quantum technology may even be eligible for that General License if they are newly hired.
- Addition of License Exception Implemented Export Control ("IEC") to authorize exports and reexports to specified destinations that have implemented similar controls to the United States. Such destinations and eligible items are identified on a list published on BIS's website, and eligible ECCNs will also state "IEC: Yes" in the ECCN's list-based license exception paragraph.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

3. Validated End User Program

In September 2024, BIS announced the expansion of its Validated End User ("VEU") program. The VEU program authorizes exports of covered items to pre-vetted end users in certain countries without a separate license required for each export, thereby expediting the export process for identified VEUs. Under the resulting October 2024 final rule, existing VEU authorizations remain available, but data centers in most countries (excluding Country Group D:5 countries) can now apply to be validated end users for exports of specified SME and advanced computing items. The new Data Center VEU program was created to ease the export and reexport burden associated with certain items controlled on BIS's Commerce Control List ("CCL")—including certain advanced computing items, but excluding "600" series items and items controlled for missile technology or crime control reasons—to pre-approved, trusted end users. As outlined in the final rule describing these changes, unlike pre-existing General VEU authorizations, in-country transfers among Data Center VEUs of items exported under a Data Center VEU authorization are not permitted. Requests for Data Center VEU authorization must be submitted via an advisory opinion request to BIS, and such a request must disclose a significant amount of information, as described in 15 C.F.R. Part 748, Supplement No. 8, such as: the proposed VEU candidate's ownership structure; the list of items for intended export; intended end users; recordkeeping practices; physical and logical (i.e., data) security requirements; current and potential customers; an overview of the data center's information security plan; an explanation of the network infrastructure and architecture and service providers; an overview of the supply chain risk management plan, export control training program, and compliance program procedures; as well as a legally binding agreement to permit U.S. Government officials to conduct on-site reviews. Upon review of an application, the End-User Review Committee ("ERC")—an interagency panel consisting of representatives of the U.S. Departments of Commerce, State, Defense, Energy and, where appropriate, the Treasury—will consider a range of national security factors and may impose conditions upon granting the authorization, such as restricting access to the facilities and limiting the computing power of a given facility. End users that meet Data Center VEU authorization requirements are listed in 15 C.F.R. Part 748, Supplement No. 7 , along with the eligible destinations and items. Even if a VEU is approved, however, exporters must obtain certifications from the VEU prior to export, provide the VEU with a written notification of the shipment containing specific details as outlined in 15 C.F.R. § 748.15(g), file semi-annual reports with BIS, and retain all relevant records for a period of at least five years. Likely due to the extensive pre-authorization requirements and substantial ongoing compliance obligations, no Data Center VEU authorization has been publicly granted to date. BIS further amended its Data Center VEU authorization, imposing additional security requirements among other changes, in a January 2025 interim final rule on AI discussed further below.

4. Advanced Semiconductors for Military Applications

In December 2024, BIS unveiled a new set of expansive regulations that the agency described as having been "designed to further impair the [PRC's] capability to produce advanced-node semiconductors that can be used in the next generation of advanced weapon systems and in artificial intelligence . . . and advanced computing, which have significant military applications." The accompanying interim final rule imposed broad new controls on SME and advanced computing items, implemented new Foreign-Direct Product ("FDP") rules—which extend U.S. jurisdiction to foreign-made items that are the "direct product" of controlled U.S.-origin technology or software, or of a manufacturing facility or equipment derived from such controlled U.S. technology or software—and further revised the EAR to clarify the scope of related controls as follows:

- New and revised ECCNs control certain SME equipment (including certain etch, deposition, lithography, ion implantation, annealing, metrology and inspection, and cleaning tools), software tools for developing or producing advanced-node

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

integrated circuits, high-bandwidth memory stacks, electronic computer-aided design software and technology, and technology computer-aided design software and technology.

- Two new FDP rules extend the scope of the EAR to include certain foreign-manufactured items that (1) are the direct product of, (2) are the product of a complete plant or major component of a plant that is itself the direct product of, or (3) contain a product of a complete plant or major component of a plant that is a direct product of, specified U.S.-origin software or technology. This third prong, capturing items "containing" a component that is a foreign direct product of U.S. software or technology, is a novel expansion of the FDP rule that as a practical matter renders such components ineligible for *de minimis* treatment when assembled into items produced abroad. From a policy perspective, these new rules are aimed at combatting efforts by the PRC to obtain foreign-manufactured SME and advanced computing items as follows:
    - The new SME FDP rule applies to certain foreign-manufactured SME and related items whenever an exporter has "knowledge," as defined under the EAR to cover actual knowledge and an awareness of a high probability, which can be inferred from acts constituting willful blindness, that a covered item is destined to a Country Group D:5 destination or Macau.
    - Similarly, the new Footnote 5 FDP rule applies to specified foreign-manufactured items used to produce advanced-node integrated circuits whenever an exporter has "knowledge" that the item will be (1) incorporated into any part, component, or equipment produced, purchased, or ordered by any Entity List entity with a Footnote 5 designation or (2) when any such designated entity will be a party to a transaction involving the commodity (e.g., as a purchaser, intermediate consignee, ultimate consignee, or end user). BIS notes that the new Footnote 5 designation is calculated to help industry identify foreign parties involved in supporting the PRC's efforts to produce advanced-node semiconductors, including for military end-uses. A companion final rule added 140 new entities to the Entity List and modified 14 existing entries, resulting in a total of 16 entities with the new Footnote 5 designation.
- Adds corresponding licensing requirements to Parts 742 and 744 of the EAR to restrict the export, reexport, and transfer of items within the scope of the new FDP rules discussed above and the new and revised ECCNs discussed above, though certain exceptions are available, including for countries implementing equivalent controls listed in 15 C.F.R. Part 742, Supplement No. 4.
- Revises the De Minimis rule—which allows foreign-made items that incorporate less than a certain *de minimis* amount of controlled U.S.-origin content to be exempt from most U.S. export restrictions—to specify there is no *de minimis* level for certain SME and advanced computing items that contain a U.S.-origin integrated circuit whenever such items are destined for a Country Group D:5 destination or Macau or to a Footnote 5 Entity List entity. These new provisions ensure that foreign-produced SME containing U.S.-origin integrated circuits (or other components) are controlled to the same extent as foreign-produced SME containing items controlled by the SME FDP rule and the Footnote 5 FDP rule.
- New License Exception Restricted Fabrication Facility ("RFF") permits the export of certain legacy SME and related items to certain fabrication facilities subject to end-user requirements, provided that these facilities are not engaged in the production of advanced node integrated circuits. Eligibility for License Exception RFF is tied to specific entities on the Entity List that contain a reference to 15 C.F.R. § 740.26, and its use is subject to various notification and reporting obligations as stipulated in that section.
- New License Exception High-Bandwidth Memory ("HBM") authorizes the export of certain HBM commodities controlled under the new ECCN 3A090.c under a narrow

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

set of circumstances, provided that specified recordkeeping and notification requirements are met.

- Eight new red flags were added to BIS's "Know Your Customer Guidance" in 15 C.F.R. Part 732, Supplement No. 3 concerning due diligence efforts that must be undertaken by exporters in various scenarios before SME and advanced computing items subject to the EAR may be exported. In particular, Red Flag 26 and the accompanying text in the interim final rule make clear the sweeping implications of the new FDP rules. In Red Flag 26, BIS notes that, due to the prevalence of U.S.-origin tools in the global production of integrated circuits, exporters should operate under the presumption that any integrated circuit is likely produced from controlled U.S. software or technology. Thus, if a foreign-produced item is described in the relevant Category 3B ECCN and contains at least one integrated circuit, there is a presumption that the product meets the product scope of the applicable FDP rule. Accordingly, an exporter must resolve this red flag before proceeding with the transaction.
- Clarified end-use controls related to the development and production of advanced-node integrated circuits, the definition of "advanced-node integrated circuit," certain general prohibitions, and a temporary general license authorizing the export of certain less-sensitive SME and advanced computing items to account for the new controls.
- Clarified that software license keys (e.g., software used to activate or renew licenses to access certain software or hardware) are classified and controlled under the same ECCNs as the software or hardware to which they provide access (or the corresponding software ECCN, in the case of access to hardware). For example, if a software license key provides access to ECCN 5A992 hardware, the key itself is classified under ECCN 5D992.

5. Mature-Node Semiconductors

In December 2024, BIS released its long-awaited Public Report on the Use of Mature-Node Semiconductors, concluding a process that began in January 2024. The report aimed to provide an overview of the use of mature-node semiconductors in supply chains that support U.S. critical infrastructure. The report based its findings on data collected from a sample of industry participants and highlighted the lack of visibility into semiconductor supply chains and the pervasive use of semiconductors manufactured by foundries located in the PRC—even though semiconductors represent a limited share of the total number of chips used in specific products. The report also highlighted how the expansion of production capacity in the PRC is beginning to impact the competitive position of U.S. chips in the global market.

6. Artificial Intelligence

The rapid rise and proliferation of artificial intelligence led the U.S. Government to implement sweeping export control regulations on AI technologies. The rules were so sweeping that they gave rise to unprecedented complaints from both U.S. hardware and software providers, as well as core U.S. allies, that the regulations were so draconian as to limit their ability to actually work on AI in manner that would be fast enough to compete with the technology emerging from China. With respect to the regulations, in a break from the hardware-based controls on the semiconductors and semiconductor manufacturing equipment necessary to *produce* an AI application or large-language model, BIS in September 2024 proposed its first rule directly regulating AI itself. The basis for this rule was unusual for BIS: Executive Order 14110, which was issued by President Biden in October 2023 to implement the Defense Production Act of 1950 (a Korean War-era statute that authorizes the President to ensure the supply of materials and services for the national defense of the United States). Consequently, the proposed rule focused on

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

gathering information necessary to protect U.S.-origin AI products or to ramp up defense industry production of such products, rather than controlling the export of any commodities, hardware, or software. The rule would require companies, individuals, or other organizations or entities that acquire, develop, or possess a potential dual-use foundation AI or large-scale computing cluster to file a quarterly report with BIS regarding any such acquisition, development, or possession, including the existence and location of clusters and the amount of total computing power available in each cluster. This reporting requirement includes information regarding the characteristics, safety (e.g., self-replication or propagation constraints, constraints on use to influence real or virtual events, constraints on ability to use the model to develop, produce, or use weapons of mass destruction), reliability, training, and cybersecurity protections of the models and regarding ownership and protection of model weights. Notably, the rule defines a "dual-use foundation model" as a model that is "trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters." This framing significantly limits the scope of covered models. BIS followed up on January 13, 2025 by issuing an interim final rule on AI diffusion, which aims to maintain U.S. technological leadership over AI by reducing diversion of advanced AI models to Country Group D:5 destinations (which, as noted above, include China and Hong Kong) and Macau, and to support development of these models in validated entities in a small set of partner countries, where they will be stored under stringent security conditions. Notably, this rule requires a license to export, reexport, or transfer (in-country) advanced computing integrated circuits or the model weights of the most advanced AI models to *any* end user in *any* destination. In particular, it controls the export of model weights for advanced, closed-weight dual-use AI models trained on more than 10^{26} computational operations in a new ECCN 4E091, as well as the export of large clusters of advanced computing integrated circuits (which can support such models) in modified ECCNs 3A090.a and .z and 4A090.a and .z. (The model weights for open-weight models do not presently require a license, and the rule also does not impose new controls on application programming interfaces to access AI platforms.) BIS also provided guidance to exporters who need assistance self-classifying their models. The rule focuses on model weights, rather than the models themselves, because model weights are more challenging to develop, require extensive model training, and are easy to copy and steal. Model weights with fewer than 10^{26} computational operations are already widely published and therefore hard to control. There is, however, a recognition that the pace of technological development may render these various weights quickly out-of-date. The U.S. Government will review applications for controlled exports, reexports, and transfers (in-country) based on the sensitivity of the destination, the quantity of compute power or performance of the AI model, and the security requirements agreed to by the recipient. The rule establishes a licensing policy of presumption of denial for both model weights and certain large quantities of advanced computing integrated circuits needed to train advanced AI models. Moreover, foreign-produced model weights of similarly advanced closed-weight models may also be controlled by this rule, through a new foreign direct product rule in 15 C.F.R. § 734.9(*l*). BIS expects such models to be subject to the rule, as it has "found that many foreign entities that are training advanced AI models or intend to train such models are using advanced computing [integrated circuits] and related items that were directly produced with U.S. technology." Despite the rule's stringent licensing policy, BIS permits certain exports to proceed by providing:

- License Exception Artificial Intelligence Authorization ("AIA") authorizing the export, reexport, or transfer of both advanced integrated circuits and model weights to end users located anywhere other than Country Group D:5 or Macau if they are employed by an entity headquartered in destinations where (1) the government has implemented measures with a view to preventing diversion of advanced AI technologies, and (2) there is an ecosystem that will enable and encourage firms to use advanced AI models for activities that may have significant economic benefits. BIS and partner agencies have listed approved countries in paragraph (a) to 15

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

C.F.R. Part 740, Supplement No. 5. Notably, that list does not include all members of the Global Export Control Coalition, which has partnered together to implement "substantially similar" controls on Russia, nor does it include all countries eligible for License Exception IEC, described above. Instead, it presently covers only Australia, Belgium, Canada, Denmark, Finland, France, Germany, Ireland, Italy, Japan, Netherlands, New Zealand, Norway, Republic of Korea, Spain, Sweden, Taiwan, the United Kingdom, and the United States. Even within these countries, exporters and reexporters may not take advantage of this exception unless they ensure that the end user has instituted specific security measures that will reduce the risk of diversion, specified in 15 C.F.R. Part 748, Supplement No. 10, and exporters of advanced integrated circuits must first obtain a compliance certification from the ultimate consignee.

- License Exception Advanced Compute Manufacturing ("ACM") authorizing the export, reexport, or transfer of items controlled by the rule to private sector end users located outside of and not headquartered in (or with an ultimate parent company headquartered in) Country Group D:5 or Macau, for the development, production, or storage of the same kinds of items (when ultimately not destined to Country Group D:5 or Macau)—but not for any other activity, including training an AI model. Parties who use this license exception are expected to keep up-to-date inventory and distribution records.
- License Exception Low Processing Performance ("LPP") authorizing the export and reexport of certain advanced integrated circuits with low computational power—up to 26,900,000 Total Processing Performance ("TPP") of advanced computing integrated circuits per-calendar year, in aggregate across all exporters for that year, to any individual ultimate consignee located outside of and not headquartered in (or with an ultimate parent company headquartered in) Country Group D:5 or Macau. Because this license exception covers the total amount of TPP an end user can receive in a year from all exporters and reexports, before using License Exception LPP, the exporter or reexporter must obtain (and ultimately provide to BIS) a certification from the ultimate consignee that the ultimate consignee has not received an aggregate of 26,900,000 TPP during the relevant calendar year and that the requested TPP for that specific transaction will not result in the ultimate consignee exceeding the TPP limit.
- An expanded License Exception ACA, which now authorizes the export and reexport of covered items to any destination worldwide other than Country Group D:5 or Macau (or to related entities), and not just to destinations in Country Group D:1 or D:4.
- A clarification of the questions BIS uses as its review criteria for License Exception NAC, which allows shipment of some advanced integrated circuits to Macau and Country Group D:5 with advanced notice to the U.S. government.
- An expanded validated end-user status for data centers—now covering both "universal" validated end users and "national" validated end users, though there is a cumulative maximum installed base allocation of 790,000,000 TPP per year for each destination country, regardless of the number of validated end users in that country. Universal validated end user ("UVEU") status will be limited to companies headquartered in or whose ultimate parent is headquartered in destinations specified in paragraph (a) of 15 C.F.R. Part 740, Supplement No. 5, and an approved UVEU cannot transfer or install more than 25 percent of its total AI computing power (i.e., the AI computing power owned by the entity and all its subsidiary and parent entities) to or in locations outside of countries listed in paragraph (a) to Supplement No. 5 to Part 740, and cannot transfer or install more than seven percent of its total AI computing power to or in any single country outside of those listed in paragraph (a) to Supplement No. 5 to Part 740. Additionally, a UVEU headquartered in the United States cannot transfer or install more than 50 percent of its total AI computing power outside of the United States. National validated end user ("NVEU") status will be available to end users in other

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

countries (except Country Group D:5 or Macau) with export limitations set on a per-company, per-country basis. Information required to be submitted to become a VEU is described in 15 C.F.R. Part 748, Supplement No. 8.

In addition, deemed exports and deemed reexports to persons employed by entities headquartered in or with an ultimate parent headquartered in this same approved country list (in paragraph (a) to 15 C.F.R. Part 740, Supplement No. 5) are not licensable. Notably, as both AI-focused rules were promulgated under multiple authorities—including E.O. 14110, which has since been rescinded by President Trump—we anticipate that any final rule, though still likely aligned with Trump administration priorities regarding the containment of China, could be subject to delay or reconsideration in light of the rules' shifting legal foundation.

7. Advanced Computing Integrated Circuits

Immediately following the expansive new regulations targeting AI discussed above, BIS on January 16, 2025 issued another interim final rule further restricting the worldwide export, reexport, and transfer of the most advanced integrated circuits classified under ECCN 3A090.a. That rule allows BIS to meticulously map global supply chains involving advanced integrated circuits through a combination of enhanced export restrictions, lists of authorized recipients for certain highly controlled items, and a quarterly reporting requirement for "front-end fabricators." BIS touted the rules, which set a compliance date of January 31, 2025, as providing clearer guidelines for conducting due diligence to confirm that an integrated circuit does not meet the parameters of ECCN 3A090.a, as well as offering a method for combatting false representations from certain end users in restricted destinations. However, the rule's complex compliance requirements will require affected companies to closely review their supply chains and third-party partners to ensure existing policies comport with the new restrictions. Key aspects of the rule include:

- Creation of a rebuttable presumption that integrated circuits meeting the parameters of ECCN 3A090.a exported by a front-end fabricator or outsourced semiconductor assembly and test ("OSAT") company are designed and marketed for data centers and therefore subject to a worldwide licensing requirement. This license requirement can only be overcome by the front-end fabricator or OSAT in one of three ways:
    - The item is destined for an approved integrated circuit designer listed in 15 C.F.R. Part 740, Supplement No. 6—which presently includes 33 U.S. Government-approved integrated circuit designers headquartered in a Country Group A:1 or A:5 destination or Taiwan—or an authorized integrated circuit designer that meets certain eligibility requirements;
    - The item is packaged by an approved OSAT company listed in 15 C.F.R. Part 740, Supplement No. 7—which presently includes 24 U.S. Government-approved OSAT companies not located in a Country Group D:5 destination—who must attest that the transistor count of the final integrated circuit is below the relevant performance threshold; or
    - The item is packaged by a front-end fabricator not located in a Country Group D:5 destination or Macau and the fabricator verifies that the transistor count of the final integrated circuit is below the relevant performance threshold.
- Development of an extensive vetting process and listing renewal process to update and revise the approved entities included in 15 C.F.R. Part 740, Supplements No. 7 and 8, described above.
- Modification of License Exceptions AIA and ACM to limit their use to approved or authorized integrated circuit designers listed above to comport with the new rebuttable presumption with respect to ECCN 3A090.a and to address diversion

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

concerns.

- Implementation of quarterly reporting requirements for front-end fabricators of integrated circuits meeting the parameters of ECCN 3A090.a, including completion of a required "Know Your Customer" vetting form by authorized integrated circuit designers. OSATs are not currently subject to this quarterly reporting requirement, but BIS noted in the interim final rule that it is evaluating extending this requirement in the future.
- Extension of the Footnote 5 FDP rule and the De Minimis rule to bring within the scope of the EAR specified foreign-manufactured items destined for a facility in a Country Group D:5 destination or Macau where the production of advanced-node integrated circuits occurs (or when an entity located at such a facility is otherwise party to the transaction), even if the entity is not designated with a Footnote 5 on the Entity List—making the Footnote 5 list non-exhaustive.

This interim final rule was accompanied by the addition of 16 Chinese and Singaporean entities to the Entity List with a Footnote 4 designation for "supporting or directly contributing to the development of advanced computing integrated circuits" in China.

B. Russia and Belarus

The United States, in parallel with efforts to restrict China's access to advanced technology, in 2024 continued to expand and refine export controls targeting Russia to stanch the flow of goods, software, and technology that can be used by the Kremlin to prosecute the war in Ukraine. Since Moscow launched its full-scale invasion in February 2022, BIS has placed wide-ranging controls on thousands of items destined for Russia and Belarus, though BIS's recent efforts have principally focused on fine-tuning these restrictions to apply even greater pressure on Russia and its allies. In January and April 2024, BIS expanded the product scope of the Iran FDP rule, which was initially implemented in February 2023 in response to Iran's ongoing military support for Russia. The February 2023 rule specifically targeted items that could be used to create unmanned aerial vehicles sent by Iran to Russia by covering foreign-produced items in categories 3 through 5 or 7 of the CCL destined for Iran, and by covering certain foreign-produced EAR99 items based on their six-digit Harmonized Tariff Schedule ("HTS") codes when destined for Russia, Belarus, or Iran. The April 2024 expansion covered 39 additional foreign-manufactured items, identified by their six-digit HTS codes, thereby expanding controls over the entirety of the Common High Priority List. (The Common High Priority List is a set of items deemed by the United States, the European Union, Japan, and the United Kingdom to present especially high risk for diversion due to their potential use in Russian weapons systems.) These items are now subject to a licensing requirement whenever they are intended for export or reexport to Iran, Russia, Belarus, or the Crimea region of Ukraine. In advance of a G7 summit in June 2024, BIS released an even more expansive list of controls by adding 522 items to the lists of items subject to Russian and Belarusian industry sanctions, resulting—together with prior controls—in license requirements for all HTS codes listed in 18 additional chapters of the HTS. These new controls, which we describe in detail in an earlier client alert, also imposed restrictions on certain riot control agents, implemented broad restrictions on certain types of EAR99 software when destined to or within Russia or Belarus, narrowed the scope of commodities and software covered by License Exception Consumer Communications Devices ("CCD") for Russia and Belarus, and added new parties—and certain addresses that present heightened diversion risks—to the Entity List for supporting Russia's military efforts. BIS described these efforts as being aimed at preventing distributors and transhippers from aiding Russia's military-industrial base, including by separately informing over 130 distributors of additional restrictions on shipments to Russia. Underscoring the extent of interagency collaboration to address Russia's malign activities, the new EAR99 software controls apply to the same types of business software covered by OFAC's June 2024 determination prohibiting the exportation to Russia of certain information technology and software services. However, the breadth of these controls is somewhat mitigated by exclusions for (1) entities engaged exclusively in the agriculture or

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

medical industries and (2) entities wholly owned by companies headquartered in the United States and certain closely allied countries, as well as joint ventures involving U.S. entities and/or entities from the same closely allied countries. In July 2024, BIS again expanded its Iran FDP rule pursuant to the No Technology for Terror Act to cover items in categories 3 through 9 (rather than only items in categories 3 through 5 or 7) of the CCL, when destined to Iran. The July rule also added a new end-user scope to the Iran FDP rule that applies when the exporter has knowledge that the Government of Iran is a party to any transaction involving the foreign-produced item. In August and November 2024, BIS took further action by imposing license requirements on the export of software and software updates for the operation of computer numerical control machine tools (including software embedded in such tools), expanding the renamed Russia/Belarus-Military End User and Procurement FDP rule to include items destined for Russian and Belarusian procurement entities designated on the Entity List with a Footnote 3 designation wherever located (thereby subjecting such foreign-manufactured items to the licensing requirements of the EAR), imposing new controls on nine chemical precursors used in riot control agents and chloropicrin (which, according to the U.S. Government, have been used by Russia as a chemical weapon in Ukraine), and explicitly expanding the availability of License Exception ENC and the exclusions for EAR99 software for the official business of diplomatic or consular missions of governments listed in Country Groups A:5 and A:6 (i.e., U.S. allies and partners). Despite imposing heavy restrictions on the flow of many items to Russia and Belarus, BIS has simultaneously sought to ensure that exports of medicine and medical equipment can proceed. In line with OFAC's Russia General License 6D, which authorizes most U.S. nexus transactions related to the production, manufacturing, sale, transport, or provision of medicine or medical devices, BIS in April 2024 introduced License Exception Medical Devices ("MED") to authorize exports of EAR99-designated "medical devices" and related items to Russia, Belarus, and certain regions of Ukraine that would otherwise be restricted by 15 C.F.R. Part 746, Supplement No. 4. Previously, many such items were subject to a licensing requirement, though BIS noted such license applications were generally approved. Importantly, License Exception MED does not authorize exports to restricted parties, to production facilities, or whenever the exporter has knowledge that the item is intended to develop or produce any items. Parts, components, and related items for medical devices may only be exported on a one-to-one basis to replace broken or nonoperational equivalent items, or because they are necessary and ordinarily incident for preventative maintenance. Despite these limitations, BIS anticipates that License Exception MED will significantly reduce the number of license applications related to medical devices and address ongoing humanitarian needs in affected destinations.

C. Multilateral Controls

As noted above, the Biden administration was heavily focused on moving away from unilateral sanctions and export controls and toward a multilateral system of regulations. This focus expanded following Russia's full-scale invasion of Ukraine. Since then, the United States has frequently turned to its partners to implement similar export controls across many jurisdictions. Importantly, recognizing that using existing multilateral control regimes was either impractical or impossible (if certain member states were less willing to go along with U.S. wishes), these more recent efforts have been pursued on an *ad hoc* basis among like-minded countries and outside the bounds of the conventional agreements that have been built up over decades. In April 2024, BIS issued an interim final rule amending the EAR to remove license requirements, expand the availability of license exceptions, and reduce the scope of end-use and end-user-based license requirements for exports, reexports, and transfers (in-country) to or within Australia and the United Kingdom as part of the AUKUS security partnership. The rule specifically focuses on significantly decreasing licensing burdens related to BIS-controlled military items, missile technology, and so-called hot section items for the development, production, or overhaul of commercial aircraft engines, components, and systems. BIS also made a notable advancement when, in October 2024, the agency promulgated an interim final rule that reduces license requirements on less-sensitive items related to spacecraft to reflect the United States' close relationship with certain countries. Specifically, the rule eases

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

requirements for items related to remote sensing and space-based logistics, assembly, and servicing of spacecraft to better rationalize the controls and facilitate collaboration among the United States, Australia, Canada, and the United Kingdom. These two actions taken together demonstrate BIS's efforts to refine export controls, including in the defense and space sectors, to facilitate collaboration and decrease regulatory friction among like-minded nations, while further distancing itself, and these technologies, from nations with interests adverse to those of the United States.

D. End-Use and End-User Controls

In addition to novel measures such as stringent controls on semiconductors and supercomputers, the United States over the past several years has used traditional export controls such as the Entity List to limit dealings involving end uses and end users of concern, with China-based organizations a perennial focus of such restrictions. As noted in our 2023 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. In 2024, BIS continued to aggressively leverage the Entity List and expanded its scope through new rules, like the addition of address-only entries. At the same time, BIS overhauled certain military, intelligence, and law enforcement end-user controls, significantly broadening the reach of these restrictions.

1. Notable Entity List Designations and Removals

Entities are added to the Entity List by the interagency End-User Review Committee. Designations occur when the ERC determines that the entities pose a significant risk of involvement in activities contrary to the national security or foreign policy interests of the United States. The evidentiary threshold for inclusion is "reasonable cause"—far below the "beyond a reasonable doubt" standard used in U.S. courts during criminal proceedings—yet the consequences can be severe. Through Entity List designations, BIS prohibits the export of specified U.S.-origin items to designated entities without BIS licensing, and BIS generally adopts either a policy of denial or *ad hoc* evaluation for license requests. 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 to, and to otherwise continue dealing with, those added to the list in transactions that do not involve items subject to the EAR or certain categories of restricted U.S.-person-provided services. The ERC has over the past several years steadily expanded the bases upon which companies and other organizations may be added to the Entity List. Further expanding the Entity List's reach, a final rule released in June 2024 authorizes BIS to add mailing addresses to the Entity List without corresponding entity names to combat unlawful diversion by shell companies that change identities to evade export controls. As such, an export license requirement now applies to all items controlled on the CCL or listed in 15 C.F.R. Part 746, Supplement No. 7 when destined to any entity using a listed address, whether or not the entity is named on the Entity List. Moreover, even when a mailing address is not listed as a standalone entry, BIS considers a party's use of the same address as a listed entity to be a "red flag," requiring businesses to undertake sufficient due diligence to ensure that co-located entities are not listed entities or acting on their behalf. Pursuant to the new "address only" rule, BIS in June 2024 added to the Entity List eight addresses and five entities in China (which includes Hong Kong under the EAR). In August 2024, BIS added three more addresses in China and one in Turkey and, in October 2024, added further addresses in China linked to significant transshipment of sensitive goods to Russia and entities at risk of violating the EAR. These address-only listings suggest BIS is focused on the use of shell companies to evade export controls, and we expect more addresses to be added to the Entity List in the future. In December 2024, BIS again broke new ground in its use of end-user controls by designating to the Entity List three China-based firms for making *investments* in semiconductors, citing their role in

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

aiding the PRC's efforts to acquire entities with sensitive semiconductor manufacturing capability with the objective of relocating these entities to China. Those designations were part of a wave of additions to the Entity List in which the United States, in a single day, curbed exports to 140 companies, including PRC semiconductor fabrication facilities and equipment manufacturers. Removals from the Entity List, on the other hand, remain rare given the requirement of a unanimous vote by the ERC. However, in October 2024, BIS, in conjunction with the U.S. Department of State, announced the removal of Canada-based application and network intelligence firm ***Sandvine Incorporated*** ("Sandvine") from the Entity List. The company was added to the Entity List in February 2024 on the basis of its products having been used for mass web-monitoring, censorship, and targeting human rights activists and dissidents. The removal followed Sandvine's structural overhaul to address the misuse of its technology, including exiting non-democratic countries and adding human rights experts to its new leadership team, and offers an illustrative example of the extensive behavioral changes and remedial measures that can persuade U.S. authorities to reconsider a party's inclusion on the Entity List.

2. Military, Intelligence, and Security End-Use and End-User Controls

In addition to broadening its use of the Entity List, BIS in July 2024 announced a proposed rule that would significantly expand existing military and military intelligence end-user controls to a broader set of intelligence end users (no longer just *military* intelligence end users), military-support end users, and—in a separate rule—foreign-security end users, including police and security services at all levels of government "with the authority to arrest, detain, monitor, search, or use force in the furtherance of their official duties" and related parties like forensic labs, prisons, detention facilities, and labor camps. These rules implement provisions of the National Defense Authorization Act for Fiscal Year 2023 and further underscore the Biden administration's emphasis on placing "human rights at the center of [U.S.] foreign policy." As described in more detail in an earlier client alert, the proposed rules broaden restrictions under 15 C.F.R. § 744.21 on "military end users" and "military end uses." Currently, the EAR prohibits the unlicensed export, reexport, or transfer (in-country) of certain items subject to the EAR to Myanmar (also called Burma), Cambodia, China, Nicaragua, or Venezuela whenever the exporting party has "knowledge" that the item is intended, entirely or in part, for a military end use in one of these destination countries or a military end user of one of these countries, wherever located. Covered items are listed in 15 C.F.R. Part 744, Supplement No. 2. In addition, military end-use and end-user restrictions currently apply to all items subject to the EAR when intended for end uses or end users located in Russia or Belarus (and to certain Russian/Belarusian entities located outside of Russia or Belarus, identified by a Footnote 3 designation on the Entity List). The proposed changes would extend these prohibitions to cover *all items subject to the EAR* (including even low-sensitivity EAR99 items) to all countries specified in Country Group D:5 (i.e., a list of arms-embargoed countries that encompasses each of the jurisdictions that is presently subject to the Military End Use / End User ("MEU") rule, plus many more) and Macau whenever the exporter has "knowledge" that the item is intended, entirely or in part, for a "military end use" or a "military end user." Those terms would be redefined to include both traditional and non-traditional military actors and to encompass end uses involving defense articles and "600" series foreign items that are not themselves subject to the EAR. Additionally, BIS would no longer list military end users on its non-exhaustive MEU List. Rather, all such entities would be transferred to the Entity List with either a Footnote 3 (for Russia/Belarus military end users subject to additional restrictions) or a Footnote 5 designation (for all other military end users). (If a final version of this rule is ultimately published, we anticipate that BIS would replace the "Footnote 5" designation with another number, as BIS elsewhere indicated that the agency would use Footnote 5 for parties involved in semiconductor manufacturing and advanced-node integrated circuit production.) These July 2024 rules would also create or enhance restrictions on U.S. person support for these revised categories of end users. In particular, where U.S. persons previously could not provide support to military end users, going forward they would be unable to provide support to a broader universe of foreign-security end users,

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

military-production activities, or to military-support end users to the extent identified within the end user's Entity List entry. Military production activities include activities to develop or produce dual-use items which, if located in the United States, would be subject to the EAR, for the benefit of a military end user, but they do not include activities that are governed by the U.S. International Traffic in Arms Regulations ("ITAR"). The restriction on providing support to military-support end users replaces previous restrictions on supporting a military end use, where that end use could include support, which is calculated to reduce the research burden on exporters. Together, these restrictions would prohibit a U.S. person from facilitating a foreign-security, military, or military-support end user's acquisition, procurement, repair, or maintenance of foreign-origin dual-use items. These U.S. person restrictions would not, however, cover provision of "published"trans technology or software that is otherwise excluded from the scope of the EAR, administrative services, commercial activities by common carriers to move goods (with some limitations), or U.S. Government activities.

3. Harmonization of BIS's Entity List and OFAC's SDN List

In March 2024, BIS announced end-user controls on entities named to OFAC's SDN List under 11 additional sanctions programs, bringing the total number of sanctions programs subject to such restrictions to 14. These new controls apply a licensing requirement for all items subject to the EAR when exported to an individual or entity designated to the SDN List pursuant to certain U.S. sanctions authorities related to Russia's invasion of Ukraine, terrorism, weapons of mass destruction, or narcotics trafficking or other criminal networks. These same restrictions apply whenever a covered SDN is a party to a transaction (i.e., as purchaser, intermediate consignee, ultimate consignee, or end user). In the final rule, BIS characterized these additional controls as a "backstop" to restrict activities otherwise not subject to OFAC jurisdiction and as a complement to OFAC's prohibitions on the provision of "material support" to blocked persons. As a practical matter, these new controls restrict non-U.S. parties from engaging in transactions with certain OFAC-sanctioned persons whenever items subject to the EAR (including by application of one or more FDP rules) are involved. The controls also have the potential to impact organizations' voluntary disclosure analyses as some transactions could now, depending upon the particular facts and circumstances, warrant parallel disclosure to both OFAC and BIS.

E. Compliance Expectations

1. U.S. Infrastructure as a Service Providers

In January 2024, BIS published a proposed rule that would require U.S. Infrastructure as a Service ("IaaS") providers (also known as cloud services providers) to collect, verify, and maintain identifying information about foreign customers of their IaaS products. Specifically, under the proposed rule, IaaS providers and their foreign resellers would need to verify the identity of foreign customers by maintaining a customer identification program. Additionally, U.S. IaaS providers would be required to file a report with BIS when they have knowledge of any transaction which results or could result in the use of their products for large AI model training. Further, the proposed rule would allow BIS to prohibit or impose certain conditions on IaaS transactions in certain jurisdictions or with specific foreign customers found to be directly supporting the use of U.S. IaaS products in malicious cyber-enabled activities. The proposed rule is based on two authorities, Executive Order 13984 signed by President Trump in January 2021, and Executive Order 14110 signed by President Biden in October 2023—the latter of which President Trump rescinded on the opening day of his second term. Consequently, a final rule could be delayed by the need to reassess the parameters of the IaaS reporting program. As we describe in a separate client alert, there are a number of practical steps IaaS providers can take to prepare for the regulations potentially becoming effective, including: reviewing and enhancing current customer identification and verification

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

practices; taking stock of foreign resellers and foreign customers; and identifying AI-related accounts.

2. Boycott Requester List

In March 2024, BIS announced the creation of the Requester List, a new online resource for antiboycott compliance. The Requester List is a public repository of entities that have made a boycott-related request that has been reported to BIS. This list is intended to assist companies, financial institutions, freight forwarders, individuals, and other U.S. persons in complying with U.S. antiboycott laws set forth in Part 760 of the Export Administration Regulations. Crucially, absent some other prohibition, U.S. persons are not restricted from engaging in dealings with entities identified on the Requester List. Rather, the list puts U.S. persons, and foreign persons subject to the reporting requirements imposed by Part 760 of the EAR, on notice that identified parties may be at elevated risk of making reportable boycott-related requests. Parties may be removed from the Requester List by submitting an attestation to the BIS's Office of Antiboycott Compliance that they will remove all boycott-related requests from purchase orders, contracts, requests for purchase, letters of credit, or other communications with U.S. persons, including with foreign subsidiaries of U.S. persons. In that sense, publication of the Requester List also appears be calculated to incentivize parties that historically have made boycott-related requests to alter their behavior going forward.

3. Financial Institutions and General Prohibition 10

In October 2024, BIS issued guidance to financial institutions detailing best practices for compliance with the EAR, and specifically with General Prohibition ("GP") 10. As we explain in more detail in an earlier client alert, GP 10 is a broad restriction on knowingly facilitating a violation of the EAR. GP 10 creates a special regulatory risk specifically for financial institutions acting as intermediaries by prohibiting the financing or servicing of an item subject to the EAR "with knowledge that a violation of the EAR has occurred, is about to occur, or is intended to occur in connection with the item." This risk has increased for financial institutions following Russia's full-scale invasion of Ukraine in 2022 and the subsequent expansion of U.S. export licensing requirements to cover broad new categories of items, including items that did not previously require financial institution scrutiny. Due to the EAR's broad jurisdictional scope, GP 10 can reach the activities of financial institutions globally, even when the parties to a transaction may not themselves be U.S. persons. The October guidance aims to help financial institutions avoid violations of GP 10 by highlighting best practices for adoption. Key compliance practices suggested by BIS include:

- Reviewing customers and their counterparties against BIS's restricted party lists, and lists of entities that have shipped Common High Priority List items to Russia since 2023, at onboarding and during risk-rating reviews;
- Obtaining export compliance certifications;
- Reviewing transactions on an ongoing basis for "red flags," including by conducting post-transaction reviews, to avoid financing or servicing a transaction going forward with "knowledge" (including imputed knowledge) of a violation, as prohibited by GP 10; and
- For certain transactions (such as cross-border payments that are likely to be associated with exports from the United States), real-time screening against certain BIS-administered restricted party lists (such as the Denied Persons List, certain persons on the Entity List, and certain military intelligence end users identified in the EAR), which generally restrict access to any item subject to the EAR.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

F. Voluntary Self-Disclosures

In addition to setting heightened expectations concerning export controls compliance, multiple agencies, including the U.S. Department of Justice's National Security Division ("NSD") and BIS, during 2024 sought to incentivize companies to submit voluntary self-disclosures ("VSDs") upon becoming aware of possible export controls violations.

1. U.S. Department of Justice Enforcement Policy

In March 2024, NSD—which, among other things, handles criminal enforcement of U.S. sanctions and export controls—announced an updated Enforcement Policy for business organizations. The policy articulates NSD's treatment of voluntary self-disclosures related to potentially criminal violations of such laws, as well as potential violations of other criminal statutes related to national security (which are often seen alongside violations of sanctions and export controls), such as money laundering, bank fraud, and false statements. Since 2016, NSD has maintained a policy encouraging industry to voluntarily self-disclose potentially criminal violations of these laws. That policy was previously updated in 2019 and 2023 to clarify incentives for disclosing companies and to emphasize that self-disclosure to a civil administrative agency (such as BIS, OFAC, or the U.S. Department of State's Directorate of Defense Trade Controls) would *not* qualify as a disclosure to NSD. The March 2024 updates to NSD's Enforcement Policy principally involve extending DOJ's Department-wide guidelines for VSDs in the context of mergers and acquisitions (the "M&A Policy") to export controls and sanctions. Under the M&A Policy, companies that undertake a lawful, bona fide acquisition of another company and, through due diligence before or shortly after the transaction, identify potential criminal violations of export control, sanctions, or "other laws affecting U.S. national security" by the acquired company, may qualify for the protections of the M&A Policy by submitting a VSD, fully cooperating, and timely remediating the misconduct. Those protections include a presumption that DOJ will decline to prosecute the acquirer and will not seek criminal fines or forfeiture. Under the M&A Policy, self-disclosure will generally be considered "timely" if made within 180 days after the transaction is completed, and any appropriate remediation should generally be completed within one year. The Enforcement Policy notes that NSD will be guided by similar principles when considering corporate criminal prosecution arising from violations of similar national security laws, including the Foreign Agents Registration Act, laws prohibiting material support to and financing of terrorists, and laws and regulations administered and enforced by the Committee on Foreign Investment in the United States ("CFIUS" or the "Committee"), or the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (commonly referred to as Team Telecom).

2. BIS Voluntary Self-Disclosures

BIS, in a September 2024 final rule, also updated its process for evaluating VSDs from industry, revising prior rules in order to give the agency additional leeway to impose higher civil monetary penalties, impose non-monetary penalties even absent a fine (e.g., suspended denial orders), and incentivize companies to disclose "significant" violations of the EAR. The rule codified updates that were announced by BIS since 2022 via a series of internal memos, made available to the public, and made additional changes. Notably, BIS amended the EAR's Penalty Guidelines to make the following changes, which we discuss in more detail in a separate client alert:

- Streamlining self-disclosure of minor or technical violations by creating a dual-track system for processing VSDs;
- Facilitating corrective action that might otherwise be prohibited by easing the ability to obtain authorization to return items to the United States that have been illegally exported;

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- Further incentivizing VSDs by treating a deliberate decision by a firm *not* to disclose a significant apparent violation to be an aggravating factor when determining what administrative penalty should be applied;
- Enhancing BIS's discretion in assessing penalties when warranted by removing prior caps on penalties, removing pre-set mitigation credit percentages, and allowing BIS to impose non-monetary penalties for non-egregious conduct that has not resulted in serious national security harm yet nonetheless merits a stronger response than a no-action or warning letter;
- Explicitly adding as an aggravating factor transactions that enable human rights abuses; and
- Motivating compliance-minded firms to report violations committed by *other* firms or competitors in order to create a "level playing field" for responsible corporate actors.

BIS also announced the appointment of the agency's first Chief of Corporate Enforcement, who will serve as the primary liaison between BIS special agents, the Department of Commerce's Office of Chief Counsel for Industry and Security, and DOJ with the aim of advancing significant corporate investigations.

G. BIS Enforcement Trends

BIS in 2024 entered into ten settlement agreements with business entities for export control violations, resulting in a combined total of approximately $10.5 million in civil penalties against six companies. The largest such penalty, a $5.8 million fine, was issued in August 2024 to a Pennsylvania-based electronics producer to resolve allegations that the company exported entirely EAR99 items to restricted end users, including five parties on the Entity List, and for restricted end uses in China. BIS also announced four antiboycott settlements during 2024 that resulted in combined civil penalties of around $400,000. BIS enforcement activity this past year focused in particular on several key sectors, including freight forwarding, electronics, and industrial products, with companies that export semiconductors and related items seemingly subject to heightened scrutiny. Key themes of BIS's published enforcement actions during 2024 included:

- BIS's commitment to imposing stiffer consequences under its new enforcement guidelines, as well as the impact of aggravating factors such as end uses and end users of significant concern;
- The expanded compliance burden on manufacturers of even low-sensitivity EAR99 items, which are now swept up in expanding export controls targeting China, Russia, Belarus, Iran, and other jurisdictions;
- The compliance considerations that should attend the use of distributors, including validation of end users and end uses, attention to payment flows, and awareness of BIS's guidance regarding "red flags"; and
- The critical role of accurate transaction screening systems and the importance of ensuring all parties involved in the supply chain and all relevant data fields are properly vetted.

In addition to entering into settlement agreements to resolve alleged violations of its regulations, BIS also showed a continued willingness to impose denial orders, which are one of the agency's most stringent enforcement measures. 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. Accordingly, a denial order—which results in the target being

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

added to the Denied Persons List—is an especially powerful tool as, in the case of a non-U.S. person, it completely severs their access to the U.S. supply chain. In one colorful case, BIS in June 2024 imposed a denial order against an Oregon-based package forwarding company for continued violations of the EAR and for failure to adhere to a prior settlement agreement, illustrating the potentially severe consequences of repeated non-compliance with BIS regulations. In that case, the denial order was initially a suspended penalty under the terms of a 2021 settlement between the company and BIS. However, when the company failed to halt the shipment of items clearly marked as export controlled and requiring an export license, BIS lifted the suspension, imposed a denial order, and barred the company for a period of three years from participating in any export from the United States or any reexport of an item subject to the EAR. Businesses should therefore be mindful that failure to abide by the terms of a settlement agreement can result in severe monetary and non-monetary penalties, up to and including the possibility of a denial of U.S. export privileges. With President Trump's first term as a guide, we anticipate that aggressive enforcement of U.S. export controls will continue under the second Trump administration. China appears to be a near-certain target of additional export control measures as the Trump administration pursues strategic competition with Beijing. Further, the America First Trade Policy Memorandum that the President signed on his first day in office specifically calls on the Secretaries of State and Commerce to review the U.S. export control system in order to advise on modifications in light of developments involving strategic adversaries or geopolitical rivals. This directive includes instructions to identify and eliminate "loopholes" in existing export controls and to make recommendations regarding "enforcement mechanisms to incentivize compliance by foreign countries, including appropriate trade and national security measures." As described at length in two prior client alerts, we expect the second Trump administration to take a number of actions in this space, including a continued and enhanced focus on restricting exports of "emerging technologies" to China, as well as maintaining the United States' relative advantage in certain key technologies such as AI and quantum computing. Secretary of Commerce nominee Howard Lutnick has made clear that robust export enforcement will be a priority. **III. U.S. Foreign Investment Restrictions**

A. Inbound Investment

In addition to sanctions and export controls, the Committee on Foreign Investment in the United States—the interagency panel tasked with reviewing the national security risks associated with foreign investment in U.S. companies—remained active and aggressive during 2024. While the total number of CFIUS filings was down from 2023, the Committee enhanced its review of non-notified transactions (i.e., transactions that are potentially within CFIUS's jurisdiction for which the parties have not filed a voluntary notice), monitored a significant number of mitigation agreements (i.e., deal-specific restrictive covenants upon which CFIUS often conditions its approval of transactions), and imposed a record number of penalties for violations of its regulations. Underscoring the Committee's heightened focus on enforcement, CFIUS expanded its monitoring and enforcement authorities in 2024 through the promulgation of a new rule increasing maximum penalties and enhancing the Committee's power to obtain information from parties with knowledge of a foreign direct investment transaction.

1. CFIUS Annual Report

In July 2024, CFIUS published its annual report to Congress detailing the Committee's activity during calendar year 2023 (the "CFIUS Annual Report"). As noted in a prior client alert, key CFIUS-related developments include:

- The total number of CFIUS filings decreased for the first time since the passage of the Foreign Investment Risk Review Modernization Act ("FIRRMA"), the 2018 statute that greatly expanded the types of transactions potentially under the Committee's purview. While the downturn in the global mergers and acquisitions market was largely responsible for this decrease, the mounting burden and cost of

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

CFIUS review, along with the increased risk of mitigation measures for even minority investments, may also be increasingly a concern for parties when assessing whether to make a voluntary filing.

- CFIUS redoubled its efforts to review non-notified transactions, including, as discussed below, by expanding its subpoena authority to request information from parties involved in non-notified filings. CFIUS also issued a rare agency-submitted notice in 2023, underscoring its power to conduct unilateral reviews of transactions when parties forgo—or refuse to re-file—voluntary filings.
- While the total number of filings decreased in 2023, CFIUS announced that it was monitoring a record-high 246 mitigation agreements.
- As we note in an earlier client alert, CFIUS imposed a record number of civil monetary penalties for breaches of material provisions in mitigation agreements in 2023, followed in 2024 by a $60 million civil monetary penalty for breach of a mitigation agreement—the largest-ever penalty issued by CFIUS.
- Finally, the CFIUS Annual Report noted the Committee's expanded jurisdiction, particularly for real estate transactions, which we discuss below.

2. CFIUS Penalties

Shortly following publication of the CFIUS Annual Report, the Committee in August 2024 provided an update on civil monetary penalties issued in 2023 and 2024. In a banner year for enforcement, CFIUS during 2024 assessed a record number of penalties, in amounts ranging up to a staggering $60 million. In a statement accompanying the penalty update, Assistant Secretary for Investment Security Paul Rosen warned: "In the last few years, CFIUS has redoubled its resources and focus on enforcement and accountability, and that is by design: if CFIUS requires companies to make certain commitments to protect national security and they fail to do so, there must be consequences."

Snapshot of CFIUS Penalties in 2024

On August 14, 2024, CFIUS shared an update on penalties issued in 2023 penalty in CFIUS's history, and the first penalty for material misstatement CFIUS filings. Importantly, also for the first time in its history, CFIUS publi involved in one of these matters, which is noteworthy as CFIUS filings and CFIUS anticipated the questions this development raises about its confide in its update that in situations where (1) there is public disclosure of CFIUS assesses public disclosure serves broader enforcement and national secu determine it is appropriate to disclose more information. We suspect the p pursuant to the terms of a settlement with the U.S. Government. In its upda new penalties assessed in 2024:

Amount	$8.5 Million	$1.25 Million
Violation	Breach of agreement	Material misstatemen
Snapshot of Violation	Majority shareholders caused removal of independent directors, leading to vacancy of CFIUS-mandated Security Director position, and causing government security committee to be defunct, resulting in failure to perform required compliance oversight.	Forged documents ar signatures, as well a material misstatements the joint voluntary notice supplemental informat submitted to CFIUS du their review, impairin CFIUS's ability to asse transaction risk.

3. Expanded Monitoring and Enforcement Authorities

In addition to vigorous monitoring and enforcement in 2023 and 2024, CFIUS also

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

broadened the scope of its oversight and strengthened its ability to impose penalties, mitigation agreements, and other enforcement measures. In April 2024, the U.S. Department of the Treasury, as chair of CFIUS, issued a proposed rule to update CFIUS's monitoring and enforcement authorities. The Committee then published a final rule in November 2024, which, as we note in a separate client alert, largely retained the proposed rule's provisions with several minor, but notable, additions. Key elements of the final rule, which went into effect on December 26, 2024, include:

- The final rule expands the scope of information that CFIUS can request in non-notified transactions, reflecting the Committee's continued attention to such transactions. Under the new rule, CFIUS can issue subpoenas not only to determine whether a non-notified transaction constitutes a "covered transaction," but also to determine whether a transaction meets the criteria for a mandatory declaration or implicates national security concerns. Moreover, CFIUS can subpoena transaction parties and other parties with knowledge relevant to the transaction, which has substantially increased its ability to gather information about transactions it believes may be subject to review.
- The final rule increases CFIUS's ability to require information from relevant parties post-review. CFIUS can now require parties to provide information to monitor compliance with or enforce the terms of a mitigation agreement, order, or condition. Additionally, CFIUS can require parties to provide information to ascertain whether the parties made material misstatements or omissions during the Committee's review of the transaction.
- In addition to strengthening CFIUS's monitoring and information-gathering capabilities, the final rule enhances the Committee's enforcement powers, most notably by sharply increasing the civil monetary penalties that CFIUS can impose, as summarized below:

Violation	Former Maximum Civil Monetary Penalty	New Maximum Civil Monetary Penalty	Other Key Changes
Material misstatements and omissions in submissions	$250,000 per violation	$5,000,000 per violation	The new rule expands penalty coverage for materi misstatements and omissions in responses to (1) CF requests for information ("RFIs") related to non-notif transactions, (2) RFIs related to monitoring and compli and (3) other CFIUS RFIs such as agency notices
Failure to submit mandatory declarations	The greater of $250,000 or the value of the transaction	The greater of $5,000,000 or the value of the transaction	CFIUS can impose the newly increased maximum pena only for violations that occur as of the effective date o rule (i.e., December 26, 2024), but also for violations re from transactions entered into or consummated prior t effective date.
Material mitigation agreement violations (intentional or through gross negligence)	The greater of $250,000 per violation or the value of the transaction	The greater of $5,000,000 per violation or the value of the transaction	"Value of the transaction" now means the greater of (1 value of the person's interest in the business at the tir the transaction or (2) at the time of the violation, or (3 value of the transaction as filed with CFIUS.

- Finally, the rule alters the time for parties to respond to mitigation agreement proposals. As a general matter, parties are subject to a very aggressive timeframe—they have three business days to provide substantive responses to the terms of a mitigation agreement. However, they may be granted more time at the discretion of the CFIUS Staff Chairperson based on factors set out in the final rule, which include the statutory deadline and parties' overall responsiveness to the Committee, as well as the national security risk arising from the transaction.

The November 2024 final rule enhances CFIUS's ability to monitor and enforce foreign direct investment compliance and suggests that, despite the change in administration, the Committee is likely to continue (if not expand) its aggressive oversight and enforcement of foreign investment controls in the coming year.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

4. Expanded Jurisdiction Over Real Estate Transactions

In December 2024, CFIUS began enforcing its final rule, published in November 2024, that expands the Committee's jurisdiction over certain real estate transactions involving foreign persons. CFIUS's Part 802 real estate regulations outline the Committee's jurisdiction over "covered real estate transactions" involving a foreign person purchasing, leasing, or gaining certain other land rights in property within specified proximities to military installations and other sensitive areas. These areas are grouped within four "Parts" outlined in Appendix A to Part 802 of the Committee's regulations. The final rule made the following updates:

- Expanded CFIUS's jurisdiction over real estate transactions to include 40 new military installations (bringing the total to 162) in Part 1, which covers real estate within "close proximity" to a listed military installation (i.e., within one mile);
- Expanded CFIUS's jurisdiction over real estate transactions to include 19 new military installations (bringing the total to 65) in Part 2, which covers real estate within the "extended range" of a listed military installation (i.e., up to 100 miles);
- Moved eight military installations from Part 1 to Part 2;
- Removed one installation from Part 1 and two installations from Part 2 due to their being located within other listed locations;
- Revised the definition of the term "military installation" to bring it in line with existing terms and the locations covered; and
- Updated the names of 14 installations and the locations of seven others.

Since the CFIUS real estate rules first became effective in 2020, CFIUS has conducted very few reviews of "covered real estate transactions." CFIUS's annual report to Congress for calendar year 2022 provided data showing that only one of the 286 notices and five of the 154 short-form declarations for that period were for covered real estate transactions. In 2023, two of the 233 notices and three of the 109 short-form declarations were for covered real estate transactions. The primary reason for the limited real estate filings is that most transactions that involve sensitive real estate are notifiable and reviewable under the Committee's Part 800 regulations addressing "covered investments." Not every covered real estate transaction poses a risk to U.S. national security and, even when CFIUS does identify a threat, in many cases the threat can be mitigated through manageable conditions on the foreign investor's physical access to, and use of, the land. As such, we do not expect the overall number of real estate reviews to rise substantially due to this new rule. We do, however, expect CFIUS to closely scrutinize the more limited universe of transactions that implicate covered real estate—regardless of whether those transactions result in voluntary filings with the Committee—and to take bold action with respect to such transactions when warranted by national security concerns. For example, in May 2024, President Biden ordered Chinese-owned ***MineOne Partners Limited*** and affiliated companies to divest recently acquired real estate within "close proximity" to Warren Air Force Base in Wyoming. This action brought renewed public scrutiny to foreign person acquisitions of U.S. real estate located near U.S. military installations and other sensitive sites.

5. State Law Investment Restrictions

In addition to conducting CFIUS-focused risk analysis, transaction parties must consider state and local foreign investment reviews—at least for now. According to one recent study, approximately 20 states have implemented some form of restriction on foreign investment in real estate, and over a dozen states are considering bills that would establish similar restrictions. Many of these state-level restrictions are currently being challenged in court. For example, in February 2024, the U.S. Court of Appeals for the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Eleventh Circuit granted an injunction pending appeal to two plaintiffs challenging a Florida law that bars 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. The Court reasoned that the plaintiffs showed a "substantial likelihood of success on their claim that [the Florida law is] preempted by federal law, specifically" FIRRMA—the statutory authority that delegates the power to regulate foreign investment in real estate to CFIUS. In a concurring opinion, one of the three panel judges suggested that plaintiffs also have a strong Equal Protection claim. 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, state 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. These state measures add another complexity to the various restrictions at the federal level targeting trade and financial flows with China and other sensitive jurisdictions. For now, at least, international investors and multinational businesses must consider not only federal law when undertaking real estate transactions within the United States, but also state-specific restrictions that may impact their commercial engagements and exposure in the United States.

6. Prospects for CFIUS Reviews and Enforcement

Despite significant leadership turnover, we assess that substantial changes to CFIUS's processes or enforcement focus are unlikely during the year ahead, though the new administration's CFIUS priorities remain unclear. Both President Biden and President Trump during his first term adopted an aggressive posture toward Chinese investment into the United States, and the second Trump administration appears set to continue, and perhaps even intensify, this approach. In addition to a harsh climate for Chinese investment, we have seen—for many years—bipartisan calls to closely scrutinize Chinese investments in agricultural land near military bases. While sweeping changes to CFIUS's regulations and practices seem unlikely, there may be some shifts in the Committee's priorities during the year ahead. For example, during the Biden administration, CFIUS increased scrutiny of investments from Saudi Arabia and other Middle Eastern government investors. Under President Trump, who previously enjoyed a close relationship with Riyadh, that trend may change. Indeed, it is noteworthy that President Trump's first call with a foreign leader following his inauguration was with the Kingdom's *de facto* ruler, Crown Prince Mohammed bin Salman; President Trump subsequently touted the Saudi leader's promise to invest $600 billion in the United States over the next four years. A second area of potential change concerns the personnel and potential politicization of CFIUS. Some observers cast the Biden administration's order blocking ***Nippon Steel***'s acquisition of ***U.S. Steel*** as an example of CFIUS decision-making being driven by political, rather than solely national security, considerations. It is unclear if CFIUS's decisions will now more closely reflect certain political inclinations of the Trump administration. Newly confirmed Treasury Secretary Scott Bessent is a former hedge fund manager, whose public comments on the role of CFIUS have been minimal.

B. Outbound Investment

After years of discussions and attempts to impose restrictions on how U.S. persons deploy capital abroad, the Biden administration in October 2024 published a final rule restricting outbound investments ("covered transactions") by U.S. persons into certain companies owned by, or affiliated with, Chinese persons (such companies, "covered foreign persons") in the semiconductors and microelectronics, quantum information technology, and AI sectors. The regulations, which became effective on January 2, 2025, divide covered transactions into three categories:

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

- Prohibited;
- Requiring notification to the newly created Office of Global Transactions within the U.S. Department of the Treasury; or
- Permitted under the various exceptions and carveouts provided in the regulations, with no further process required.

As we note in a prior client alert, while the outbound investment regulations have effectively created a new trade controls regime from scratch—and indeed, there is much that is truly novel in the regulations—they nonetheless draw heavily on existing processes, definitions, and penalties that will be familiar to sanctions, export controls, and CFIUS practitioners. As with CFIUS, the penalties for violations of the outbound investment regulations are steep. Importantly, these regulations rely upon the same statute that authorizes almost all U.S. sanctions programs—the International Emergency Economic Powers Act ("IEEPA"). Consequently, the penalties for violations are the same. In particular, the Treasury Department may impose civil penalties of up to twice the value of the underlying violative transaction. Willful violations can result in criminal penalties of up to $1,000,000, imprisonment for up to 20 years, or both. The outbound investment regulations apply globally to U.S. persons making certain acquisitions of equity in covered foreign persons, including contingent equity, equity-type rights, and joint ventures. Unlike CFIUS, the outbound investment regulations also apply to greenfield investments. The restrictions also extend to foreign entities that are controlled by a U.S. parent, requiring the U.S. parent to take all reasonable steps to prevent any transaction by its controlled foreign entity that is prohibited under the outbound investment regulations. U.S. persons are further prohibited from "knowingly directing" transactions by non-U.S. persons that would be prohibited for a U.S. person to conduct itself. Foreign subsidiaries of U.S. companies, however, are not necessarily subject to the regulations. Covered foreign persons include not only entities that have their principal place of business, headquarters, or place of formation in China, but could also include entities with Chinese ownership and deemed control. In that sense, even though the outbound investment regulations are focused solely on China (including Hong Kong and Macau), their applicability is global. The outbound investment regulations include a long list of exceptions from coverage to address industry concerns. For example, unless the investment affords the U.S. person rights beyond "standard minority shareholder protections," a term that remains mired in some ambiguity, investments by U.S. persons in publicly traded securities (including on non-U.S. exchanges) or a security issued by an investment company (such as an index fund, mutual fund, or exchange-traded fund) are excepted, as are certain limited partner investments. Certain intracompany transactions between a U.S. parent and a controlled subsidiary are also permitted. The regulations further include an exception for certain transactions involving countries that have enacted similar outbound investment restrictions in national security technologies, which is noteworthy as the European Union has already taken material steps toward developing their own regime. As described in a separate client alert, the Treasury Department in December 2024 published Frequently Asked Questions ("FAQs"), as well as guidance on the national interest exemption whereby the U.S. Government may, upon request, determine that a covered transaction is in the U.S. national interest and is therefore exempt from the outbound investment restrictions. More FAQs followed in January 2025 and Treasury launched a new website with enforcement guidelines and instructions for submitting notifications and requests for exemptions. Although the outbound investment regulations are still in their infancy, investors have undertaken various measures to promote compliance, including:

- Enhancing internal due diligence programs to identify whether potential investments involve prohibited or notifiable technologies, including by assessing specific design elements and end uses of technologies and products, as well as determining whether AI systems were trained using certain levels of computing power;
- Seeking binding contractual assurances from investment targets that the capital invested will not, directly or indirectly, create a notifiable or prohibited transaction;

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

and

- Establishing processes whereby a U.S. person may recuse themselves from covered transactions in order to avoid exercising their authority to "knowingly direct" a transaction and run afoul of the outbound investment regulations.

The outbound investment regulations could soon play a meaningful, and growing, role in U.S. trade policy. Although the regulations are presently targeted at U.S. outbound investments in China, and are limited to a narrow group of critical technology sectors, the regime could easily be expanded. For example, the Trump administration could in coming months broaden the list of restricted investments to include additional sensitive sectors such as hypersonics, satellite-based communications, and networked laser scanning systems with dual-use applications. The President could also expand the countries of concern—investments to which would also be subject to these regulations—beyond China.

IV. U.S. Import Restrictions In addition to standing up a new China-focused outbound investment regime, the Biden administration during 2024 continued to restrict imports from China through vigorous enforcement of the Uyghur Forced Labor Prevention Act ("UFLPA"). Meanwhile, import actions of another sort will play an early and prominent role in President Trump's trade policy as the new administration has implemented increased tariffs of 10 percent on China and threatened (but not yet implemented) even more substantial increased tariffs of 25 percent on Canada and Mexico—among the United States' closest allies and members of the United States-Mexico-Canada Agreement (the "USMCA") signed by President Trump during his first term.

A. Uyghur Forced Labor Prevention Act

During 2024, the Biden administration sought to strengthen implementation of the Uyghur Forced Labor Prevention Act by expanding both the number of entities targeted under the law and the range of sectors identified as high priorities for enforcement. The expansion of the UFLPA also brings to light the expanded reliance by the U.S. Government on non-governmental sources of information in executing its policies and the consequent accretion of power by politically unaccountable actors in academia and the private sector in furthering government policies. This has been clear since Russia's expanded invasion of Ukraine began in 2022 (after which private sector parties have pressed for government action) and has continued in the context of the UFLPA. Interestingly, the U.S. Government has not only admitted to this involvement but has celebrated its "partnerships" with non-governmental actors. As discussed in a prior client alert, the UFLPA 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 prohibited from entry into the United States. The statute has put pressure on companies to implement effective supply chain diligence programs, tailored to meet the challenges of modern supply chains with intricate webs of sub-tier suppliers. The interagency Forced Labor Enforcement Task Force ("FLETF")—chaired by the U.S. Department of Homeland Security ("DHS"), which is the agency within which U.S. Customs and Border Protection ("CBP") resides—is charged with administering the UFLPA Entity List. Following early criticism that additions to that list needed to be expanded, particularly in the face of non-governmental and academic research identifying thousands of companies that appear to meet the UFLPA's criteria, the FLETF began designating in earnest during 2024. As of January 14, 2025, 144 entities are identified on the UFLPA Entity List—a nearly fivefold increase from the end of 2023. Notably, the vast majority of designated entities are located in areas of China other than Xinjiang, highlighting the need for effective diligence that is not solely focused on avoiding sourcing inputs and final goods directly from that region. New additions to the UFLPA Entity List have spanned a range of industries, including cotton and textiles, agriculture products, metals and mining, seafood, aluminum, and footwear. The large number of designations in the cotton sector, one of the original high-priority sectors identified for enforcement under the UFLPA, dovetails with DHS's broader strategy, announced in April 2024, to "level the playing field for the American textile industry." This also indicates the dual purpose of these restrictions—to

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

promote human rights-sensitive sourcing, while also addressing significant trade imbalances. In its annual strategy update on UFLPA implementation, DHS for the first time since 2022 formally identified new “high-priority” sectors for enforcement. The 2024 update adds aluminum, seafood, and polyvinyl chloride (“PVC”) to a list that already included apparel, cotton and cotton products, silica-based products, and tomatoes and downstream products. Each of these additions follows in-depth non-governmental organization reporting on links between those products and Xinjiang forced labor, including aluminum in automotive supply chains, PVC in vinyl flooring supply chains, and seafood destined for the United States and the European Union. Similar reporting at the end of 2024 regarding pharmaceutical supply chains may portend a future target of enforcement. In the two and a half years since the UFLPA went into effect, CBP has detained over 12,000 shipments under the law, valued at over $3.6 billion. Approximately half of those detained shipments have ultimately been released into the United States, an apparent result of successful "applicability review" submissions, whereby companies can seek the release of goods by demonstrating that they are not within the scope of the law’s prohibitions (i.e., because they are not made wholly or in part in Xinjiang or by entities on the UFLPA Entity List). The largest numbers of detentions were associated with the electronics, automotive and aerospace, and apparel, footwear, and textiles industries, per CBP’s classifications. A drop in the value, but not the volume, of shipments detained in the second half of 2024 may indicate a focus on lower-value inputs or component parts. Importantly, China has not been the leading originating nation from which detained shipments have derived. Rather, Malaysia and Vietnam have been—again highlighting the importance of supply chain diligence that goes further than merely inquiring as to the final country from which a good is exported. To further strengthen forced labor enforcement, some U.S. lawmakers have called for changes to the *de minimis* exception—a customs law provision whereby certain low-value shipments are afforded lesser scrutiny at U.S. ports of entry and on which China-based “fast fashion” retailers often rely. Although not focused on the UFLPA, CBP in January 2025 published a notice of proposed rulemaking in which the agency announced plans to amend the *de minimis* exception, noting that the existing rules make U.S. supply chains more vulnerable to “goods potentially made with forced labor.” While serving in the U.S. Senate, newly confirmed Secretary of State Marco Rubio co-authored the UFLPA and was one of the most vocal advocates in Congress for more aggressive enforcement. As such, although the State Department is not directly tasked with UFLPA enforcement, between his role as a leading member of the cabinet, the degree of broad bipartisan support for the law, and President Trump’s longstanding support for restricting Chinese imports, conditions appear to be ripe for sustained vigorous enforcement of the UFLPA throughout the year ahead.

B. Tariffs

Following years of relative quiet under President Biden, threatened and/or actual increased tariffs and trade wars have already emerged as a key part of the Trump administration’s approach to engaging on international economic and geopolitical issues. Domestically, any executive action to impose increased tariffs on goods originating from specified jurisdictions such as USMCA members (Canada and Mexico), China, or the European Union, or conceivably all goods entering the United States (collectively, the “Proposed Tariffs”), will almost certainly be the subject of substantial legal challenges, particularly as the U.S. Constitution provides that Congress has general responsibility with respect to tariffs on imports. However, as noted below, Congress since 1930 has delegated substantial authority to the President that could support executive action to increase tariffs. Accordingly, challenging the Proposed Tariffs could prove difficult, particularly those imposed pursuant to the International Emergency Economic Powers Act, which broadly authorizes the President to impose economic restrictions “to deal with any unusual and extraordinary threat . . . if the President declares a national emergency with respect to such threat.” (A somewhat analogous "international peace or security"2 exception in the USMCA could also substantially limit the prospects for success in a USMCA challenge to increased tariffs on imports from Canada and Mexico.) Despite the enhanced possibility of meaningful challenges to presidential action due to the overturning of *Chevron* deference and the emergence of the major questions doctrine, we assess that

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

in other than truly unusual matters, it is likely that courts would continue to broadly defer to the Executive in matters involving claims of national security and foreign affairs. Notably, President Trump in early February 2025 invoked IEEPA—the 1977 statute that underlies nearly all U.S. sanctions programs and which broadly authorizes the President to take action during a period of national emergency declared by the President—to announce increased tariffs on goods from Canada, Mexico, and China (with the increased tariffs on goods from Canada and Mexico paused for at least a month). While President Nixon in 1971 invoked a predecessor statute, the Trading With the Enemy Act, to briefly impose 10 percent tariffs on many goods imported into the United States, President Trump's use of IEEPA to levy increased tariffs is unprecedented. The Trump administration has nevertheless taken this step, and quickly secured at least temporary concessions from Ottawa and Mexico City that could invite further threats of IEEPA-based tariffs going forward. To the extent the White House is inclined to rely on delegations of authority other than IEEPA, there are a number of existing statutes that authorize the President to impose increased tariffs under certain circumstances that might provide support for at least some subset of the Proposed Tariffs:

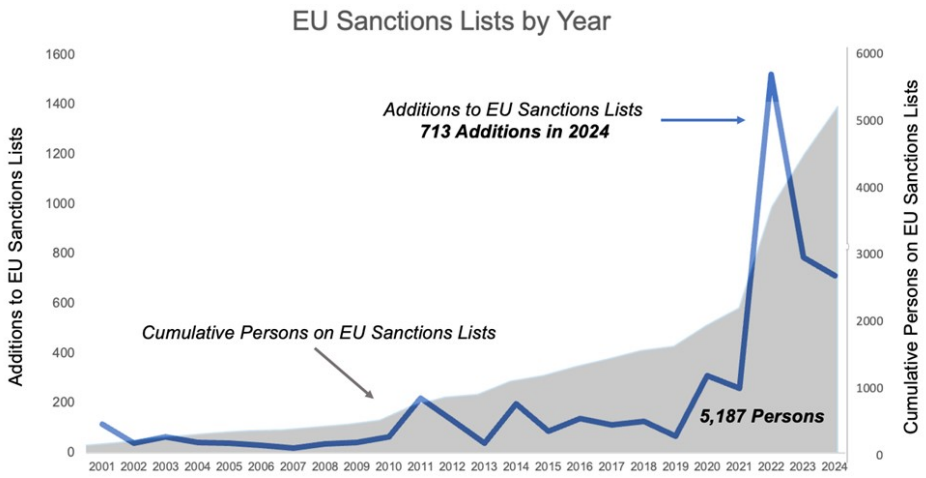
- **Section 301 of the Trade Act of 1974** authorizes the President, following an investigation and determination by the Office of the U.S. Trade Representative ("USTR"), to impose tariffs in response to acts, policies, or practices of a foreign government that either violate trade agreements or are unjustifiable, unreasonable, or discriminatory and burden or restrict U.S. commerce. While Section 301 would authorize increased tariffs on imports from particular foreign jurisdictions based on findings of unfair trade practices, it is unlikely to authorize a broadly applicable tariff on all goods entering the United States, as it requires the identification of such acts, policies, or practices by a specific foreign country. Actions taken by the outgoing Biden administration demonstrate how Section 301 could be deployed. In December 2024, USTR announced that it was initiating a Section 301 investigation "regarding China's acts, policies, and practices related to targeting of the semiconductor industry for dominance," focusing on "legacy" semiconductors. If USTR under the new administration finds unreasonable or discriminatory practices that burden U.S. commerce, President Trump may impose tariffs targeting not only Chinese legacy semiconductors but also downstream products from other nations that contain such semiconductors. This could result in even further tariffs imposed on China-origin chips, which are already slated to be subject to 50 percent tariffs in 2025.
- **Section 232 of the Trade Expansion Act of 1962** authorizes the President to impose tariffs on imports of articles determined by a U.S. Department of Commerce investigation to undermine national security, and was used by the first Trump administration to impose 25 percent increased tariffs on imports of certain steel products and 10 percent increased tariffs on certain aluminum products. Those tariffs were initially applied to imports from all countries, but were later subject to special arrangements negotiated with Brazil, South Korea, Canada, Mexico, and Argentina, and an exemption for Australia. (The Biden administration maintained those Section 232 tariffs, and reached further agreements with the European Union, Japan, and the United Kingdom.) Thus, Section 232 could be an effective tool for the Trump administration to impose (and negotiate) increased tariffs or other restrictions on particular types of goods. However, such action would be delayed by a Commerce Department investigation and would not seem to authorize a broad tariff increase on all goods entering the United States even from a single specified country, much less a broad increased tariff on all articles from all countries.
- **Section 122 of the Trade Act of 1974** authorizes the President to impose tariffs up to 15 percent for 150 days in response to "balance-of-payments deficits." Section 122 could authorize the Proposed Tariffs, but only temporarily and only for an increase of up to 15 percent.
- **Section 338 of the Tariff Act of 1930** authorizes the President to impose

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

additional tariffs of up to 50 percent against particular countries that discriminate against U.S. exports (i.e., as compared with exports from other nations). However, the statute is ambiguous on the procedures required to rely on its authorization, including the role of the U.S. International Trade Commission, an independent, bipartisan agency, in investigating the underlying trade issues and setting the tariffs. Moreover, courts have not had an opportunity to clarify such ambiguity because the statute has not been used in over 90 years. On its face, Section 338 may authorize increased tariffs on goods from particular countries, but its uncertain terms and the apparent requirement to find that the country or countries discriminate against U.S. exports would not seem to support its use to authorize a broadly applicable tariff on all goods entering the United States.

Regardless of the authority the Trump administration might use to implement the Proposed Tariffs, such actions, along with likely retaliation by foreign governments (which has already included China's addition of a major U.S.-based apparel company to a list of "unreliable entities"), would significantly impact global supply chains and could lead to decreases in the availability of certain goods and increases in the cost of goods around the world. China, Canada, Mexico, and the European Union have indicated they are prepared to retaliate should President Trump move forward with the Proposed Tariffs. Moreover, elevated tariffs on Canada and Mexico would almost certainly face legal challenges, as they may violate the United States' obligations under the USMCA, the successor to the Clinton-era North American Free Trade Agreement. Some observers have suggested that President Trump could be counting on the threat of tariffs to prompt an early re-negotiation of the USMCA, which re-negotiation is currently scheduled for 2026. Alternatively, the Trump administration, in concert with the U.S. Congress, could look to effectuate the Proposed Tariffs legislatively—something that has not happened since the Smoot-Hawley Tariff Act of 1930. Although the prospects for congressional action are at best uncertain, should such legislation be passed through the Republican-controlled Congress and signed into law, it could be exceedingly difficult to challenge the result via litigation. On balance, however, we assess it as far more likely that the President will seek to use executive actions to this end. **V. European Union**

A. Sanctions



1. Harmonization of EU Rules

As the European Union's more than 40 sanctions regimes continue to expand and grow in complexity, a fundamental challenge has emerged: inconsistent sanctions enforcement across EU Member States. During 2024, Poland and the Netherlands led the charge with 22 and 10 enforcement actions, respectively. Conversely, Lithuania imposed the most substantial sanctions-related fines of the year: €13.6 million and €9.3 million for breaches

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

of export prohibitions and the provision of crypto asset services to Russian persons. Despite such sporadic successes, these developments exemplify a growing disparity within the European Union, as over half of Member States this past year did not conclude a single successful sanctions-related enforcement action. As the lack of uniformity creates gaps that can be exploited for evasion purposes, the Netherlands has published a "non-paper" (i.e., an informal discussion document) outlining seven key reforms to strengthen sanctions implementation and enforcement across the European Union. The Dutch proposal calls for, among other things, the creation of a centralized risk assessment hub to identify circumvention risks, the allocation of resources to EU Member States to support enforcement efforts, the adoption of baseline compliance rules for high-risk, large businesses to prevent breaches of sanctions, and the expansion of data available to the European Commission (the bloc's executive branch) and EU Member States through the Sanctions Information Exchange Repository (e.g., on ownership and control structures to enable national competent authorities in Member States to make more informed and consistent licensing decisions). The Dutch non-paper, although not an official EU proposal, notably advances the debate over possible institutional reforms at the EU level. That said, the European Union in 2024 made strides toward harmonizing sanctions enforcement. While historically less than half of EU Member States criminalized sanctions violations (in the other states, it has merely been a civil infraction), during 2024 the European Union adopted a directive establishing minimum rules on the definition of criminal offenses and penalties for violations of EU sanctions. Conduct constituting a criminal offense will include asset freeze violations (e.g., making funds or economic resources available directly or indirectly to, or for the benefit of, a designated person), as well as trade sanctions violations (e.g., providing services to a designated person). Circumvention, as well as inciting, aiding, and abetting the commission of an offense, will also constitute an offense. Under the directive, fines for corporates will be able to reach one percent or five percent of annual turnover or, alternatively, €8 or €40 million, depending on the offense. A new asset freezing and confiscation regime targeting instrumentalities and proceeds of EU sanctions violations was also introduced. EU Member States have until May 20, 2025 to transpose the new rules into national legislation. To further minimize the potentially inconsistent interpretation of EU rules, the Council of the European Union (the grouping of ministers from each EU Member State that is responsible for negotiating and adopting EU legislation) issued a revised edition of its Best Practices for the Effective Implementation of Restrictive Measures. Key additions include thorough guidance on the concept of "control," which is a constituent part of the European Union's test for whether entities affiliated with sanctioned persons should be treated as sanctioned themselves. The Council's guidance identifies as possible "red flags" for control the presence of a buyback option or a transfer of shares to non-designated persons close in time to a shareholder's designation, which together suggest the level of detail that EU economic operators are expected to take into account in their diligence efforts. The exact contours of the "control" test, however, remain unclear. The European Banking Authority ("EBA") also contributed to the harmonization of sanctions rules during 2024 by issuing new guidelines that set common, EU-wide standards on the governance arrangements, policies, procedures, and controls financial institutions should have in place to comply with EU sanctions regulations. One set of guidelines applies to all institutions within the EBA's supervisory remit and sets out requirements relating to governance and risk management systems to effectively address risks of non-compliance with, or evasion of, sanctions. A second set of guidelines applies to crypto asset service providers and payment services providers and specifies what such firms should do to comply with sanctions when performing transfers of crypto assets and funds, respectively, including restricted party screening and due diligence requirements. Both sets of guidelines will become effective on December 30, 2025. The harmonization of EU sanctions rules could be further enhanced in the months and years ahead as the bloc's newly established Anti-Money Laundering Authority ("AMLA")—launched in June 2024 to supervise high-risk entities and coordinate among EU Member State financial intelligence units—begins to monitor compliance with sanctions-related measures by cross-border groups in the financial sector, and contribute to general sanctions compliance supervision. However, as AMLA will not become fully operational until 2028, it remains to be seen how the agency will interact with other supervisory and enforcement bodies across the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

European Union.

2. Russia

The European Union in 2024 adopted two new Russia sanctions packages, further targeting Russia's military, defense, energy, and maritime sectors. Key new measures in the energy sector, which remains a major source of revenue for the Kremlin, include prohibitions on providing goods, technology, or services to liquified natural gas ("LNG") projects under construction in Russia, the transshipment of Russian LNG through EU ports, and the importation of Russian LNG into specific terminals that are not connected to the EU gas pipeline network. With fewer options for new restrictions left on the table, a recurring theme of recent EU sanctions packages is a focus on anti-circumvention tools. During the past year, the European Union designated companies actively involved in the evasion of EU sanctions. Entities incorporated and/or operating in transshipment hubs such as China, Kazakhstan, Turkey, the United Arab Emirates, and India were added to the list of entities associated with Russia's military-industrial complex, subjecting them to stricter export restrictions. As we note in an earlier client alert, the European Union also introduced a "best efforts" obligation on EU parent companies to ensure that their non-EU subsidiaries do not take part in activities that undermine EU sanctions. While that measure does not expand the jurisdictional reach of EU sanctions legislation, and therefore does not impose obligations on foreign entities, it is a consequential development in the fight against circumvention as it attempts to leverage EU corporate influence abroad in order to further the impact and effectiveness of sanctions measures (much as the United States has done for decades). Although a definition of "best efforts" is not included in binding legislation, the European Commission has suggested in public guidance that such actions may include the implementation of internal compliance programs, systematic sharing of corporate compliance standards, sending newsletters and sanctions advisories, setting up mandatory reporting, or organizing mandatory sanctions trainings for staff—all practices which European companies are encouraged to adopt. We assess it as likely that President Trump will seek to end the war in Ukraine by attempting to negotiate a deal with Russia's President Vladimir Putin—and sanctions relief would undoubtedly be part of any such deal. If the United States proceeds with significantly reducing sanctions on Russia and EU Member States remain unwilling to do so, we could see a meaningful divergence between the two regimes, which would result in compliance challenges for multinationals with footprints in both the United States and Europe.

3. Development of New Sanctions Regimes

The European Union during 2024 developed new tools to tighten the screws on Moscow by introducing two new Russia-related sanctions regimes. One regime addresses Russia's destabilizing activities against the European Union and its Member States, and is designed to target parties who, for example, engage in or facilitate the use of coordinated information manipulation and interference, or who engage in or facilitate the obstruction of the democratic political process, including by undermining elections or attempting to overthrow the constitutional order. The European Commission in December 2024 designated 19 new parties under that regime, with a focus on dismantling Russian disinformation networks in Africa and Europe. As key elections are set to be held across many major states in Europe in 2025, further designations under these regimes appear likely in coming months, and could conceivably leverage a noteworthy feature of the regime that—similar to the concept of "material support" in U.S. sanctions—contemplates designating persons "supporting" parties that engage in destabilizing activities. The second new sanctions regime targets parties responsible for human rights violations, repression of civil society and democratic opposition, and the undermining of democracy and the rule of law in Russia. This regime is part of the European Union's response to accelerating and systematic repression in Russia, which included the death of opposition leader Aleksey Navalny in February 2024. Under this regime—which has similarities with the United States' Magnitsky and Global Magnitsky sanctions programs—the European

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Commission may take action against those responsible for the commission of human rights violations in Russia. To date, 20 designations have been announced under the regime, including targeting members of the Russian judiciary and the central authority managing Russia's prison system, and new trade restrictions on equipment that might be used for internal repression or for use in information security and the monitoring or interception of telecommunication have been introduced.

4. Case Law and Referrals to the CJEU

2024 was also noteworthy for a significant rise in litigation implicating sanctions provisions, as well as national courts in EU Member States referring questions relating to EU sanctions interpretation to the Court of Justice of the European Union ("CJEU"). The increasing volume of case law on EU sanctions underscores the growing complexity of this area of law, its impact on commercial transactions, and the competing imperatives that courts face in balancing EU foreign policy objectives against the rights and interests of both individuals and companies within the Union.

a) Interpretation of "Brokering Services" in Russia Regulations

The CJEU has confirmed that the prohibition on the provision of brokering services in relation to military equipment to persons in or for use in Russia applies even where the goods subject to the brokering deal are never imported into EU territory. In the Court's view, if the rule were otherwise, then the prohibition could easily be neutralized by arranging for the equipment to be routed via non-EU Member States. The Court further found that the automatic confiscation by Romanian authorities of the full payment received by the Romanian company in question for the provision of brokering services was an appropriate and proportionate step to ensure the effectiveness of the prohibitions and the deterrent effect of penalties.

b) Interpretation of Legal Advisory Prohibitions

In C-109/23, the CJEU held that notarial services do not fall within the definition of legal advice or legal advisory services under the European Union's Russia sanctions regime, on the theory that such services amount to an official state function and not a legal advisory service to an individual. The Court further noted that the term "legal advice" generally refers to an opinion on a question of law, and found support for its interpretation in the recitals to the relevant EU regulation. Separately, the General Court rejected several challenges to the legality of the legal advisory prohibition (T-797/22; T-798/22; T-828/22), holding that the prohibition is consistent with the protection of professional secrecy, the right to a fair trial, and the principle of proportionality. The CJEU's judgment in C-109/23 is also noteworthy as it is a rare instance in which the Court directly contradicted a frequently asked question published by the European Commission, which indicates that notarial services are within the ambit of the legal advisory prohibition in the Russia sanctions regulations. That split of opinion underscores that guidance issued by the Commission is not legally binding, as the CJEU is the ultimate arbiter of EU law. That said, absent judicial interpretation to the contrary, it remains good practice for persons subject to EU jurisdiction to adhere to the guidance set forth in the Commission's FAQs.

c) ECB Prudential Requirements for Russian Operations

The European Central Bank ("ECB") over the past year has been engaging with European banks with significant exposure to Russia. The ECB has set a clear roadmap for banks to downsize their operations and eventually exit from Russia. The ECB's imposition of prudential requirements on banks that continue to operate in Russia has

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

been hotly contested and has generated significant practical challenges for companies that maintain legitimate (and still legal) business ties with Russia. However, the General Court rejected an application by a major Italy-based financial institution seeking to suspend an ECB decision establishing prudential requirements on its operations in Russia, which included restrictions on the grant of new loans and deposits. The Court's reasoning focused on the risks for the bank resulting from an increasingly complex sanctions environment. The Court held that the decision by the ECB to impose such requirements was strictly within the powers conferred to it, which allow the ECB to restrict the business of institutions and/or request the divestment of activities that pose excessive risks to the soundness of an institution.

d) Referrals to the CJEU

EU Member State courts in 2024 often referred questions concerning EU sanctions regulations to the CJEU, including numerous pending queries regarding ownership and control such as:

- Whether, under circumstances in which a designated person owns exactly 50 percent of the shares in a company, the company's funds are presumptively owned or held or controlled by the designated person;
- When a legal person can be deemed to be "associated" with a designated person;
- Whether assets held in trust for a designated person can be regarded as belonging to, or being controlled by, the designated person where this is prohibited by the trust's governing law or where dealing with such assets would breach EU law; and
- Whether asset freezes mean that designated persons cannot exercise voting rights attached to depository receipts.

In December 2024, a Swedish court asked the CJEU for a preliminary ruling interpreting the "no claims" clause in the Russia sanctions regulations. As of this writing, these questions remain pending before the Court.

5. Iran

During 2024, Iran continued to threaten European security through malign activities including providing military support to armed groups in the Middle East and supplying unmanned aerial vehicles and ballistic missiles to Russia. In light of these developments, the European Union widened its new Iran sanctions regime to target vessels and ports used for the transfer of UAVs, missiles, and related technologies and components. Further designations stemming from Iran's missile transfers to Russia included the largest Iranian airline ***Mahan Air***, Iranian flag carrier ***Iran Air***, and shipping companies, including the national maritime carrier ***Islamic Republic of Iran Shipping Lines***, involved in transporting Iranian-made weapons and ammunition, including UAV components, across the Caspian Sea to resupply Russian troops. Some EU policymakers voiced concern that such measures do not go far enough in combatting the threat that Iran poses to European and international security, prompting a November 2024 European Parliament resolution calling for further sanctions. As such, a further expansion of EU sanctions targeting Iran appears likely in coming months. Of note, while there was some concern that a return to the maximum pressure campaign implemented by President Trump in his first term would result in a meaningful divergence between EU and U.S. sanctions, Tehran's continued troubling behaviors have moved the European Union much closer to the U.S. position. As such, we assess that a meaningful split between EU and U.S. sanctions on Iran—which could present substantial corporate compliance challenges—is less likely than might have been the case even a short while ago.

6. EU Member State Sanctions: Germany

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Germany in 2024 remained an especially active EU Member State in the field of sanctions implementation and enforcement as German government agencies continued to be prolific sources of guidance and unique sources of general authorizations. Notably, Berlin has issued General Licenses (i.e., regulatory exemptions) within the framework of EU sanctions, despite the European Commission disapproving of this practice in public guidance. Nevertheless, Germany's Federal Office for Economic Affairs and Export Controls (*Bundesamt für Wirtschaft und Ausfuhrkontrolle*) ("BAFA") in 2024 continued undeterred as it extended General License No. 30 for a further year to authorize eligible persons to undertake otherwise restricted yet non-sensitive transactions involving Iranian persons located or headquartered in the European Union or the United Kingdom. BAFA also adopted the first General License within the framework of EU sanctions on Russia. General License No. 42 authorizes eligible persons, until December 31, 2025, to provide otherwise restricted services and/or software for the exclusive use of non-sensitive recipients in Russia, such as subsidiaries of companies incorporated in the European Union or partner countries. Germany, across several government agencies, also continued to issue and update its independent guidance on EU sanctions, with a particular focus on Russia sanctions. For example, the German Federal Ministry for Economic Affairs and Climate Action (*Bundesministerium für Wirtschaft und Klimaschutz*) ("BMWK") updated its FAQs on Russia sanctions and issued guidance on measures to prevent diversion of military items to Russia via non-EU subsidiaries of EU companies. Meanwhile, BAFA updated its leaflet on foreign trade with Russia, and the German Federal Bank (*Deutsche Bundesbank*) updated its FAQs on EU financial sanctions, which predominantly focus on sanctions against Russia and Belarus. Germany has also continued to tighten enforcement with further development of the Central Department for Sanctions Enforcement (*Zentralstelle für Sanktionsdurchsetzung*) ("ZfS"). Established in 2023, the ZfS's primary responsibility is to enforce the prohibitions around making funds and economic resources available to designated persons, for which the agency has been granted comprehensive powers. However, some observers have questioned ZfS's capacity, as less than half of the agency's open positions have reportedly been staffed as of May 2024. In parallel, powerful Public Prosecutor's Offices, of which Germany has more than one hundred, have established themselves as an unexpected driving force behind sanctions implementation by initiating numerous criminal enforcement actions. Some Public Prosecutor's Offices have favored expansive and aggressive interpretation of sanctions regulations, considerably heightening risks for companies and individuals subject to German jurisdiction. Although criminal convictions have to date only involved individuals, German prosecutors and enforcement authorities appear poised to scale up their sanctions enforcement efforts during the coming year, with an eye toward eventually aiming for larger corporate targets. The growing body of sanctions materials from Germany has been a welcome development for many companies that have long sought more clarity on the rules and the risks of EU sanctions. However, the uncertain relationship between German rules and those promulgated by the European Commission, let alone differences between German interpretations and those of other EU countries, could portend real challenges both for the power of EU sanctions (which derives in large part from there being a unified approach among all 27 Member States) and for corporate compliance going forward.

B. Export Controls

Following the U.S. lead, the European Union in 2024 increasingly sought to restrict the export of high-tech goods that have the potential to be misused by authoritarian regimes, even as EU Member States continued to struggle toward a coordinated, bloc-wide approach to export controls. In January 2024, the European Commission published a white paper on export controls to assess whether current rules could be improved in the face of geopolitical challenges and rapid technological advances. Much as with the potential balkanization of EU sanctions enforcement (discussed above), the white paper, which was announced as part of the Union's Economic Security Strategy, identifies the fragmentation of the EU export control regime as a threat to EU economic security, as it risks creating loopholes, undermining the effectiveness of controls, and threatening the

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

integrity of the single market. The white paper points in particular to the blocking of new controls by certain Member States, the increasing use of unilateral export controls, and a lack of a single EU-wide approach as significant challenges. In response, the Commission proposed adding new items to the EU Dual-Use List, creating a high-level forum to foster a common EU position regarding export controls, improving coordination of national control lists, and bringing forward to 2025 the next evaluation of the EU Dual-Use Regulation. Member States have likewise recognized the need for greater coordination of EU export controls, with the Dutch government publishing a paper supporting the Commission's proposal. Unsurprisingly, and in line with what we have seen across the world, technological advances have regularly outpaced legislation and regulation. This has led EU Member States to deploy their own national controls on the export of high-technology goods. At times, the advent of national-level controls has been a function of U.S. diplomatic pressure directed at specific EU Member States—such as the Netherlands, which plays a uniquely critical role in the production of high-end semiconductor manufacturing equipment. At the EU level, the European Commission in September 2024 added seven types of nuclear plants and equipment, as well as additional toxins and chemical precursors, to its regulations restricting exports of dual-use items. Following the United States' lead, the Commission in October 2024 also issued new guidelines for cyber-surveillance exporters, which aim to minimize the risk of cyber-surveillance items being used for internal repression or the commission of serious violations of human rights and international humanitarian law. The guidelines require exporters to notify authorities when they learn that non-listed cyber-surveillance items are intended for use in connection with such activities. Notwithstanding these efforts to make export controls more consistent across EU Member States, some members of the bloc continued to unilaterally implement controls on dual-use goods that extend beyond those specified in the EU Dual-Use Regulation. Following Spain and the Netherlands, which had already added semiconductor manufacturing equipment and technology to their national control lists, France in February 2024 imposed controls on goods and technologies associated with quantum computing, advanced electronic components, and semiconductors, and Italy and Germany in July 2024 adopted national control lists for dual-use goods that included semiconductor manufacturing equipment, chips, and quantum computers. The uncoordinated proliferation of national export controls by EU Member States further increases the compliance burden on industry who now, even within the common market, must contend with a patchwork of local laws.

C. Foreign Investment Restrictions

1. Inbound Investment

Foreign direct investment ("FDI") activity picked up in the European Union during 2024 even as the number of formal screenings steadily increased and multiple EU Member States made moves to enact legislation or reform existing regimes. The European Commission in January 2024 issued a proposal to reform the EU Foreign Direct Investment Regulation (the "EU FDI Regulation"), which includes a requirement for Member States to enact FDI legislation—similar in spirit to the United States' CFIUS—within a 15-month timeline. Several EU Member States, including Bulgaria and Ireland, subsequently introduced FDI regimes, while Romania and France amended their existing mechanisms. This obligation will therefore principally impact Croatia, Cyprus, and Greece as they are presently the only Member States without an active regime, though all three jurisdictions have taken "concrete steps" to put a screening mechanism in place. The Commission's proposal would broaden the scope of the EU FDI Regulation to capture FDI by European entities whose ultimate owners are non-EU investors. The Commission also made strides towards greater consistency across EU Member States. Its proposal recommended both process harmonization, such as the introduction of minimum standards for screening processes, and substantive harmonization, such as a more prescriptive list of sectors and activities that will require authorization. As of this writing, the Commission's proposed reforms have yet to clear the European Parliament's legislative process, and it is uncertain when they might enter into force. In October 2024,

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

the European Commission published its fourth annual report on the application of the EU FDI Regulation, which sheds some light on key data and trends. According to the report, the European Union during calendar year 2023 experienced an increase of net FDI inflows. The United States and the United Kingdom together contributed the majority of foreign investment into the European Union at, respectively, 30 percent and 25 percent of all deals during 2023. Within the Union, Germany and Spain were the most common recipients of FDI inflows, as those two Member States attracted 19 percent and 17 percent of all deals. The volume of FDI screening across Member States also continued to increase. In 2023, 1,808 transactions were reviewed by national authorities (up from 1,444 in 2022), of which 56 percent were formally screened. However, as in prior years, the vast majority of investments were cleared unconditionally (i.e., with no required mitigation measures), with only 1 percent of transactions ultimately blocked. As such, it appears that while the number of formal screenings is increasing, the number of investments identified as posing a serious threat to security or public order remains low. While the EU FDI Regulation does not set up a system for EU-wide FDI screening, it does include a mechanism for coordinating FDI reviews to allow the European Commission, as well as other EU Member States, to issue comments and opinions on FDI transactions in other Member States. While the host Member State retains the final word, in circumstances where investments are deemed to be of EU-wide interest, host Member States are required to give careful consideration to the Commission's views and explain any departure from them. Notifications under the EU FDI Regulation's cooperation mechanism—pursuant to which EU Member States and the European Commission are able to exchange information and raise concerns in relation to specific investments—continued to increase in 2023. Sectors giving rise to the largest share of such notifications were similar to previous years, including manufacturing, information and communication technologies, wholesale and retail, financial activities, and professional activities. Of the cases referred under the cooperation mechanism, the European Commission closed 92 percent in Phase 1 (i.e., following a preliminary assessment) and issued an opinion in less than 2 percent of notified transactions. The most common ultimate origin of investors remained the United States and the United Kingdom, while the number of transactions where the ultimate investor was based in United Arab Emirates more than doubled as compared to the preceding year. Moreover, EU Member States actively enforced their FDI regimes this past year. Germany in July 2024 blocked the acquisition of ***MAN Energy Solutions*** by ***CSIC Longjiang Guanghan Gas Turbine*** due to security concerns stemming from the buyer's links to the Chinese defense industry. In August 2024, Spain issued its first-ever public veto in August 2024 to prevent the acquisition of Spanish train manufacturer ***Talgo***. This case is noteworthy as the ultimate investor was Hungarian, and Spain blocked the acquisition on the basis that it "posed risks for the country's national security and public order." This may be an indication of some political fragmentation of the bloc as some Member States, such as Hungary, have a seemingly and radically different strategic and political outlook compared with others.

2. Outbound Investment

A year after a European Commission white paper found that EU Member States do not systematically review and assess outbound investments for national security purposes, apprehension relating to possible strategic technology leaks continued. Driven by these concerns, and no doubt borrowing from the United States' outbound regime, the Commission in January 2025 published a recommendation calling on Member States to conduct outbound investment reviews in exactly the same technological sectors: semiconductors, AI, and quantum technologies. Each was identified as being of strategic importance and posing the highest national security risk. The recommendation forms part of the European Union's Economic Security Strategy, and was prepared in tandem with the Commission's ongoing work on inbound FDI screening (discussed above). Although the European Union has historically refrained from explicitly referencing China in policy papers or legislative proposals, the Union has in recent years taken legislative steps to prepare for a more antagonistic relationship with Beijing and to equip the bloc with policy tools to protect its economic security. As the recommendation is not legally binding, its

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

chief purpose is to nudge EU Member States to assess risks to economic security stemming from outbound investments made by EU investors in the three key technologies in third countries, with a view to enabling the European Commission to propose further action. That review by Member States is set to cover both ongoing and past transactions dating back to January 1, 2021. Member States are asked to, by June 30, 2026, submit to the Commission a comprehensive report on their implementation of the recommendation and any risks identified—though the European Commission is widely expected to take further steps toward standing up an outbound investment regime before that review period is complete. **VI. United Kingdom** Marking five years since Brexit, the United Kingdom has now fully developed its independent sanctions and export controls mechanisms. Similar to those across the Channel, but arguably more in line with those emerging from Washington, London has become a robust issuer and enforcer of sanctions measures, second in the world only to the United States. As it moves forward, and perhaps even more closely toward the United States, there are numerous ways in which this convergence can be seen. Growing closeness, collaboration, and cooperation between OFAC and the UK Office of Financial Sanctions Implementation ("OFSI"), information sharing with Washington (and Canberra) under AUKUS, and harmonization of certain controls are all examples of this trend toward closer alignment between the United Kingdom and its core allies. One perhaps even more significant measure relates to the use of the Pound as a medium of exchange in global transactions. While the United Kingdom has not gone as far as the United States in asserting jurisdiction over any transaction that relies on a correspondent bank, the United Kingdom has reiterated in published guidance that transactions using clearing services in the United Kingdom may establish a nexus with UK jurisdiction.

A. Sanctions

1. Russia

The UK Government in 2024 redoubled its commitment to isolate Russia economically by implementing targeted restrictive measures aimed at cutting off funding and support for Moscow's war machine. As of May 2024, the United Kingdom has sanctioned over 2,000 parties under its Russia sanctions program, including more than 1,700 designations since February 2022. Far from losing steam, the United Kingdom in November 2024 implemented its largest sanctions package of the year with the aim of further restricting the supply of equipment used by Russia's military-industrial complex and targeting Russia's global activities, in particular in Mali, the Central African Republic, and Libya. That package consisted of 56 new designations across five UK sanctions regimes. Targets included suppliers of equipment to the Russian military-industrial complex, including entities based in China, Kazakhstan, Uzbekistan, and Turkey, plus Russian-backed mercenary groups operating in sub-Saharan Africa. These new designations highlight the United Kingdom's focus on both countering Russia's extraterritorial influence and restricting the supply of goods and technology to Russia's military. While the United Kingdom and its allies have taken significant actions to sever Russia from the global financial system, limit its energy revenues, and target its military-industrial complex, Russia has employed intricate, costly strategies to bypass such measures. By developing complex supply chains through third countries to obtain restricted goods and creating parallel trade networks to maintain key exports such as oil, Russia has grown heavily reliant on external support. To deter such circumvention and evasion networks, the United Kingdom in 2024 continued to expand the criteria pursuant to which persons can be designated under its Russia sanctions program. Specifically, a person—regardless of their location or place of incorporation—may now be designated for providing financial services, or making available funds, economic resources, goods, or technology to persons involved in obtaining a benefit from or supporting the Government of Russia; and for owning or controlling, directly or indirectly, or working as a director, trustee, other manager, or equivalent of, a company involved in destabilizing Ukraine. That expansion of the United Kingdom's designation criteria brought London into closer alignment with the United States—which continues to be eager to apply its own sanctions extraterritorially or designate persons in third countries for providing material support to OFAC-sanctioned

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

parties. Within the Russia sanctions program, the United Kingdom this past year devoted considerable attention to the maritime sector. This is a logical area of focus given the importance of the United Kingdom as a center for shipping insurance and the role of some of its Overseas Territories in the broader shipping sector. Among other measures, the United Kingdom in October 2024 implemented its largest package of sanctions against Russian shipping, designating over 30 oil tankers and entities, as well as 10 vessels in Russia's so-called "shadow fleet"—an alternative ecosystem of hundreds of aging and questionably seaworthy oil tankers, backed by sub-standard insurers, that operate outside the jurisdiction of allied countries that have implemented substantially similar sanctions on Russia. Direct sanctioning of vessels is a recent innovation in the United Kingdom, as that power was only introduced in July 2024. Designating vessels has been a longstanding and effective practice in the United States, which undoubtedly provided inspiration for the United Kingdom's measures. The UK Government has also reportedly launched 37 investigations into UK-linked entities—believed to include maritime insurance firms, plus ship owners, operators, and brokers—for alleged breaches of the Russia oil price cap, though no prosecutions or fines have yet been announced. To help industry comply with sanctions on Russian shipping, the UK Government in 2024 published an unprecedented volume of industry-specific guidance, suggesting a sustained focus by London policymakers on the maritime sector. Key publications included guidance for the maritime sector generally, as well as specific guidance on tanker sales to third countries and a fact sheet on maritime shipping. Collectively, these publications call on industry participants to adopt a comprehensive approach to ensuring their compliance with UK financial sanctions that includes elements such as due diligence, use of advanced technology and screening tools, and increased collaboration. In light of the importance of oil sales and imported goods to Russia's economy, it is widely expected that shipping will continue to be a sanctions policy priority for the United Kingdom and its allies throughout the year ahead.

2. Iran

The United Kingdom in 2024 continued to tighten restrictions on Iran in response to the Islamic Republic's proliferation of advanced weaponry, aid to militant groups across the Middle East, and ongoing support for Russia's war in Ukraine. In light of these developments, the United Kingdom in September 2024 amended its Iran sanctions regime to restrict goods and technologies used in the production of ballistic missiles, UAVs, and other weaponry. The United Kingdom also imposed a series of asset freezes against parties alleged to have facilitated Iran's military support for Russia, including in November 2024 the state-owned airline, Iran Air, and the national shipping carrier, Islamic Republic of Iran Shipping Lines. Although Iran's new president Masoud Pezeshkian has expressed interest in reviving the 2015 nuclear accord between Tehran and a group of major powers, prospects for such an agreement appear remote, at least in the near term, following President Trump's return to the White House and Iran's continued human rights violations at home and regional destabilization activities abroad. Indeed, the United Kingdom could expand its measures against Iran with one option, put forward by an influential conservative think tank, involving the United Kingdom fully aligning with the U.S. sanctions regime on vessels involved in the illicit trade of Iranian oil, and coordinating with its allies to disrupt Iran's "shadow fleet" by pressuring third countries to de-flag vessels deemed to have facilitated illicit sales of Iranian crude. Although the new Labor government's foreign policy agenda continues to develop and the level of cooperation with the new Trump administration is uncertain, it appears likely that further UK restrictive measures on Iran will be imposed in the coming year, presumably in coordination with key allies.

3. Office of Trade Sanctions Implementation

In light of the growing overlap between trade sanctions and export controls as a result of the sweeping restrictions introduced under the Russia sanctions regime, His Majesty's Revenue and Customs ("HMRC") has been pursuing civil enforcement of both trade

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

sanctions and export controls. As anticipated, the United Kingdom partly relieved HMRC of that double role with the October 2024 launch of a new agency dubbed the Office of Trade Sanctions Implementation ("OTSI"). As a formal matter, OTSI will complement HMRC's powers, with HMRC retaining responsibility for criminal enforcement. However, as a practical matter, OTSI is expected to take on the bulk of the work relating to enforcement of UK trade sanctions, as most actions are taken on a civil basis. OTSI sits within the UK Department for Business and Trade and its authorities are similar to those of the Office of Financial Sanctions Implementation, including the imposition of monetary penalties and public disclosures of breaches (which OTSI assesses, like OFSI, on a strict liability basis), enforcement of reporting obligations, and extensive information-gathering powers. OTSI's ability to publicly disclose details of alleged breaches contrasts with the limited information that HMRC has historically published when it issues compound settlements, and is a welcome development to guide industry's compliance efforts. OTSI will also play an advisory and licensing role, which it promptly started serving by publishing detailed guidance on civil enforcement and the assessment of breaches, which indicate that OTSI will consider a number of mitigating factors when evaluating potential breaches, including timely and voluntary disclosure, compliance with information requests, and a business's sanctions risk profile. OTSI offers a concrete example of the UK Government's investment in sanctions implementation and enforcement. In light of the agency's specialized focus and its authority to enforce on a strict liability basis, increased civil enforcement of UK trade sanctions—especially in relation to the provision of services and circumvention schemes—appears likely in coming months.

4. Cooperation and Multilateralism

The United Kingdom has been closely coordinating with its international partners to implement and enforce multilateral sanctions. Following a flurry of coordinated designations and restrictive measures, including a joint action targeting Russian metals, the burgeoning partnership between OFSI and its U.S. counterpart OFAC marked its second anniversary in November 2024 with a joint publication on the fruits of their collaboration and a memorandum of understanding on sanctions information sharing. That memorandum is noteworthy as it sheds light on the types of documentation and intelligence that the two agencies expect to share and confirms the official, and now codified, nature of the exchange. Such collaboration was not limited to cooperation between London and Washington. In February 2024, the G7 (of which the United Kingdom is a member), plus the European Union and Australia, published an alert detailing key Russian oil price cap evasion methods and recommendations for mitigating circumvention risks. In tandem with the G7, the United Kingdom in September 2024 issued first-of-its-kind joint guidance for industry on preventing the evasion of export controls and sanctions on Russia. That same month, as part of the Export Enforcement Five, alongside Australia, Canada, New Zealand, and the United States, the United Kingdom issued a joint statement reaffirming its commitment to coordinated export control and sanctions enforcement to prevent the diversion of dual-use items that support Russia's war in Ukraine. London's approach to multilateralism is also flexible and adaptable. While coordination with allies remains a key priority, the United Kingdom could be more likely to closely align with the European Union and other core allies such as Australia or Canada during 2025 if policy differences emerge between the Starmer government and the new Trump administration.

5. Case Law Interpreting UK Sanctions

UK courts hold final authority to interpret legal texts, including UK sanctions regulations, and are being called upon with growing frequency to resolve disputes and provide clarity on matters related to sanctions implementation.

a) Ownership and Control

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Following conflicting interpretations of the "ownership and control" tests—the UK legal concept under which sanctions restrictions extend to entities that are majority-owned or controlled by a designated party, whether or not the entity itself has been explicitly identified—the High Court in July 2024 discussed "control" in more detail in *Hellard v OJSC Rossiysky Kredit Bank & Ors*. Under UK law, "control" is found when it would be reasonable to expect that a designated party would be able, if it chose to, in most cases or in significant respects, by whatever means and whether directly or indirectly, to achieve the result that affairs of a non-designated company are conducted according to the designated party's wishes. The Court in *Hellard* broke down instances of "control" into four distinct categories:

- ***De jure* control** occurs when there is a legal right to exercise control, as set out in a company's constitution or governing documents. This is established through the examination of legal instruments or foundational documents.
- **Actual present *de facto* control** refers to a situation where someone is effectively "calling the shots," even though they do not have a formal legal right to do so, which can be evidenced by showing that the putative controller is exerting decisive influence over the company's activities.
- **Potential future *de jure* control** applies when a person has the legal means to gain ownership or control in the future, such as through options or forward contracts.
- **Potential future *de facto* control** involves a situation where, although there is no present *de facto* control, it is reasonable to believe that the individual could exercise control in the future if they chose to. Such a belief could arise from specific circumstances that suggest the individual has the potential to exercise control in a manner that does not rely on a legal right or power. The Court noted that this type of control is likely rare in practice.

As such, the *Hellard* judgment provides a helpful roadmap to navigate the complexities of the notoriously opaque "control" test in UK sanctions legislation.

b) Divestment Transactions

In the Russia sanctions context, purported divestment transactions at or around the time a person becomes designated are not uncommon as parties attempt to shield entities that they own from the effect of sanctions, and often raise thorny questions regarding residual ownership and control. In *Vneshprombank LLC v Bedzhamov*, the High Court clarified that the presence of a "reasonable cause to suspect" that an entity continues to be owned or controlled by a UK-designated person, even after ownership has been formally transferred to a non-designated person, constitutes a "stepping stone" toward making a factual determination regarding ownership and control and does not, standing alone, make out the relevant offense unless the entity in question is *in fact* owned or controlled by the designated person. The *Vneshprombank* case underscores the need for businesses to carefully scrutinize any changes in ownership of entities linked to designated individuals, as a "reasonable cause to suspect" can be established even without definitive evidence that a transaction is a sham. That case also sheds light on potential "red flags" that may suggest a sham transaction, including the lack of a commercial rationale for the purchase, the timing of the transaction, the acquisition price, and the role of the acquirer prior to the imposition of sanctions. Moreover, the case serves as a notable reminder that OFSI's pronouncements are not determinative and can be overridden by the judiciary, as the Court in *Vneshprombank* expressly assigned little weight to OFSI's guidance in relation to the ownership and control tests.

c) Force Majeure

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

In the eagerly awaited case of *RTI Ltd v MUR Shipping BV*, the UK Supreme Court considered whether acceptance of non-contractual performance can overcome a state of affairs caused by sanctions, therefore preventing application of a *force majeure* clause. The shipowner involved in the dispute had invoked a *force majeure* clause following the imposition of U.S. sanctions on its parent company, which made payments in U.S. Dollars—the currency contemplated by the contract—difficult. The Court confirmed that a "reasonable endeavours" provision in a *force majeure* clause does not require a party to accept non-contractual performance, absent clear wording to that effect. As such, "reasonable endeavours" does not require a contractual party to accept payment in Euros when a contract provides for payment in U.S. Dollars, even though U.S. sanctions impacting the other party mean contractual payment in U.S. Dollars would be cumbersome or impractical. *MUR Shipping* therefore underscores the difficulty in mitigating the impact of sanctions on commercial transactions and the importance of forward-looking drafting.

d) Financing and Financial Assistance

In *Celestial Aviation Services Ltd v UniCredit Bank GmbH*, the Court of Appeal clarified four key aspects of the UK sanctions regime:

- The Court underscored the wide-reaching scope of the financial services restrictions that accompany many trade sanctions measures. Specifically, the Court of Appeal confirmed that restrictions on the provision of financing or financial assistance in relation to certain restricted items apply to exports that took place prior to the imposition of sanctions. That is, where restricted items are presently located in Russia, persons subject to UK jurisdiction are prohibited from providing ancillary services (including financial services) in relation to such items, regardless of when those items were exported to Russia. That approach aligns with the view taken by the European Commission in its published guidance.
- The Court affirmed the importance of the UK specific licensing regime, noting that the UK Government has chosen to craft restrictive measures as "blunt instruments" which "cast the net sufficiently wide to ensure that all objectionable arrangements are caught," preferring to grant authorizations on a case-by-case basis.
- The Court highlighted the breadth of the general defense to liability for actions taken due to a "reasonable belief" that such actions were necessary to comply with sanctions, thus providing reassurance to those who may abide by a conservative interpretation of sanctions prohibitions in good faith.
- Having found that the terms of the financial instrument in question did not contemplate payments in cash or any currency other than U.S. Dollars, the Court—drawing on the principle established in *Ralli Bros*—held that one of the parties had not made all "reasonable efforts" to avoid illegality, as it had only applied for a very narrow license from OFAC, which would have been unlikely to cover the dealings in question. This serves as a reminder that when parties face sanctions-related impediments to contractual performance, they should reasonably scope and calibrate proposed mitigation measures.

6. Enforcement Trends Implementation

a) Office of Financial Sanctions

Following an internal review of OFSI's procedures, the UK Government in November 2024 introduced several key amendments to strengthen OFSI's enforcement powers, equip the agency with improved intelligence on industry compliance with sanctions legislation, and streamline licensing applications. For instance, the amendments broaden the scope of financial sanctions reporting obligations by expanding the definition of relevant firms to cover high-value dealers, art market participants, insolvency practitioners,

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

and letting agencies. Those changes were prompted by suspected breaches of sanctions within some of the affected sectors that were not proactively reported to OFSI. Further, the amendments expand reporting obligations to require relevant firms to report suspected beaches of sanctions regulations, in addition to (and regardless of whether amounting to) suspected criminal offenses. Previously, relevant firms were only required to report to OFSI where they knew, or had reasonable cause to suspect, that a person committed an offense under financial sanctions legislation. This extension aligns the reporting obligations on relevant firms with OFSI's broader civil enforcement powers. These changes were accompanied by guidance for each of the newly added sectors. The UK Government in January 2025 indicated that there were at that time 318 open investigations regarding potential violations of Russia sanctions, and that 388 cases relating to potential Russia-related breaches have been closed since February 2022. This data suggests that, although the degree of regulatory scrutiny by OFSI has substantially increased, most cases do not ripen into an enforcement action. A letter from the Foreign, Commonwealth, and Development Office to the Chair of the House of Commons Foreign Affairs Committee noted that, from 2017 to March 2024, OFSI imposed ten monetary penalties, totaling £22 million—a significant achievement for the agency, but still significantly lagging its U.S. counterpart OFAC. OFSI subsequently imposed a penalty against ***Integral Concierge Services Limited*** ("Integral Concierge") in September 2024, marking the agency's first penalty in relation to Russia sanctions following Moscow's full-scale invasion of Ukraine and the first imposed on a strict liability basis. The Integral Concierge penalty notice provides insight into OFSI's compliance expectations. The agency underlined that it is essential to understand one's exposure to sanctions risks and take appropriate action to address them, and companies dealing with a high-risk client base must ensure they are thoroughly informed about the associated risks. The notice also stressed the importance of cooperation and voluntary self-disclosure to obtain a reduction in penalty.

b) Other Government Agencies

The past year offered a reminder that sanctions-related enforcement is broader than OFSI. In a rare enforcement action, the UK Financial Conduct Authority ("FCA") fined ***Starling Bank*** £29 million for systems and controls failures relating to sanctions compliance. According to the FCA, the bank allegedly failed to ensure that its financial sanctions screening systems were operating efficiently and appropriately. In its final notice, the FCA provided a practical overview of the necessary actions regulated entities should take to ensure that financial sanctions systems and controls are robust and effective. Similarly, the UK Gambling Commission, in a separate enforcement action, fined ***Bet365*** £582,120 for betting license breaches, including alleged shortcomings in its financial sanctions controls such as a failure to undertake sanctions screening checks on new customers. In a landmark development for UK sanctions enforcement, the National Crime Agency ("NCA") in July 2024 secured the forfeiture of £780,000 of sanctioned funds under the Proceeds of Crime Act 2017 in the first known NCA investigation into alleged evasion of Russia sanctions. The funds, which the NCA deemed to be held for the benefit of a designated Russian oligarch despite not being in his name, had been frozen since 2022. The two-year investigation showcases the complex, resource-intensive nature of bringing sanctions evasion cases to trial. Nevertheless, the NCA appears likely to play a pivotal role in UK sanctions implementation and enforcement going forward. Further, the UK Government during 2024 continued to collaborate across agencies to ensure cohesive implementation of UK sanctions, including through information sharing and the issuance of joint guidance. For example, in January 2024, multiple agencies, including the NCA, OFSI, and HMRC, issued an alert detailing the risks of financial sanctions evasion, money laundering, and cultural property trafficking through the art storage sector.

B. Export Controls

1. Dual-Use and Military Controls

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

The United Kingdom in 2024 followed its core allies, the United States and the European Union, in tightening protections around sensitive emerging technologies in recognition of their importance to national security. Beyond implementing in domestic legislation amendments to the Wassenaar Arrangement control lists, the United Kingdom also expanded its export control regime to include a number of key emerging technologies, including dilution refrigerators, quantum technologies, semiconductor technologies, and advanced materials. AUKUS—the trilateral security partnership among Australia, the United Kingdom, and the United States aimed at strengthening defense and security cooperation in the Indo-Pacific region—represented a historic breakthrough in defense trade. After years of negotiations, the three countries agreed to relax certain export controls and restrictions on technology sharing. As part of this collaboration, the UK Department for Business and Trade in September 2024 introduced an open general license specifically for AUKUS that facilitates the export of dual-use items, military goods, software, and technology, and trade in military goods among the three closely allied countries. To avail themselves of that license, exporters and recipients must be listed as authorized users by the AUKUS nations. Not all actions taken in the past year, however, were aimed at facilitating trade in controlled items. According to data released by the Department for Business and Trade, between September and December 2024, the United Kingdom rejected 17 military export license applications to Israel, a notable increase compared to no rejections in the preceding quarter. Sixteen of 368 active export licenses for Israel are presently suspended, including licenses for components used in fighter aircraft, unmanned aerial vehicles, naval systems, and targeting equipment. This rise in scrutiny of exports is part of a broader trend of tightening UK export controls, with refusals of standard individual export licenses reaching record levels. Separate data published by the Department for Business and Trade shows that each quarter since late 2022 has seen over 100 total refusals across all destinations, far surpassing the historical average of 74 refusals per quarter since 2008, and suggesting that close scrutiny of export licensing is likely here to stay.

2. Enforcement Trends

Although HMRC continues to monitor compliance with export control legislation, enforcement during 2024 lagged behind key allies such as the United States. HMRC offered compound settlements (i.e., civil penalties in lieu of prosecution), for a total of £1.9 million, to three exporters found to have engaged in unlicensed exports of military-listed goods and dual-use goods under the Export Control Order 2008. These resolutions followed seven settlement offers, totaling over £2.3 million earlier in the year, also relating to unlicensed exports. Despite having increased the issuance of substantial fines and reportedly aiming for larger targets, HMRC continues to abide by its longstanding practice of not disclosing the identity of parties found in violation of export control regulations, which limits industry's ability to draw lessons from enforcement actions. Nevertheless, in an effort to support UK exporters, the UK Government updated its general guidance on export controls and encouraged exporters to voluntarily disclose breaches of export controls as well as trade sanctions legislation by offering the prospect of a penalty reduction of up to 50 percent. Cooperation with HMRC remains an effective means to avoid criminal prosecution. Conversely, failure to engage in a timely and proactive manner can have tangible consequences, as when an exporter failed to respond to HMRC's compound settlement offer and was subsequently found guilty of breaching export controls (i.e., a criminal offense) and fined close to the maximum penalty available on the facts of £89,000.

C. Foreign Investment Restrictions

1. Inbound Investment

Following a sustained downward trend in inbound foreign direct investment flows, the United Kingdom adopted a more permissive approach to the application of the National

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

Security and Investment Act 2021 ("NSIA") as part of its foreign direct investment screening in 2024. Only 4.4 percent of all notifications during the year to March 31, 2024 were called in for in-depth reviews. Notably, of the 906 notifications that were submitted (up from 865 in the prior year), no transactions were blocked or unwound. Four non-notified deals were issued a "call-in notice" to respond to Investment Security Unit ("ISU") concerns about a prior transaction. Just as the ISU continued its use of call-in powers, companies also made use of retrospective validation applications under the NSIA, in which filings can be submitted after the relevant transaction has already closed, if filed during the reference period. ISU did not issue any penalties in respect of the missing filings to which these applications related. In previous years, the United Kingdom has prohibited transactions based on, among other factors, the country of origin of the acquirer. However, data from the most recent year shows that, while 41 percent of called-in transactions involved Chinese acquirers, 39 percent of called-in transactions concerned UK acquirers and 22 percent concerned U.S. acquirers. With nearly a quarter of called-in transactions related to a country of origin that has traditionally been a friend or close ally of the United Kingdom—and over a third related to domestic acquirers—this data suggests 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. This data may also suggest that the United Kingdom's focus, at least when deciding to call in a transaction, primarily depends upon the company's business activities (i.e., whether its activities fall within the 17 sensitive sectors defined under the NSIA). With respect to those sensitive sectors, the United Kingdom continued to focus in 2024 on protecting military and defense assets. Nearly 48 percent of all notifiable acquisitions concerned activities in the defense sector. The defense sector also accounted for the largest share of transactions subjected to an ISU call-in (at 34 percent), with activities in military and dual-use second (at 29 percent). The United Kingdom also continued to focus on companies active in the data infrastructure sector, having imposed requirements that such data must be solely maintained in the United Kingdom and not exported. It is also within the data infrastructure sector that the United Kingdom this past year saw its first High Court challenge of the NSIA, which remains under review. In November 2024, the High Court handed down the first-ever judgment on the application of the NSIA. With a focus on procedural aspects, the Court upheld the ISU's order that ***LetterOne***, an investment company related to Russian investors, divest ***Upp Corporation Ltd*** ("Upp"), a broadband telecommunications company. Notably, the initial Russian investors in LetterOne included individuals subject to UK sanctions due to their involvement in state-affiliated businesses and their close association with Russia's President Vladimir Putin. The ISU appears to have been concerned by the ultimate beneficial owner's susceptibility to influence from the Russian government. In particular, Upp's involvement in UK critical infrastructure, including the anticipated rollout of the company's full fiber broadband network, gave rise to national security concerns such as potential disruption of the broadband network's operations, access to customer data for espionage purposes, and influence over Upp's strategic decisions. Although this judgment serves as a reminder of the deference that the courts afford the UK Government in national security matters in keeping with the broader UK principle of separation of powers, it also sets a high bar for future challenges to decisions under the NSIA. In particular, the High Court defended decisions made by the ISU and noted that the ISU could not be reprimanded for taking preventative actions to avoid the potential risk of Russian interference with critical infrastructure and the government need not have waited for those risks to materialize. The Court also dismissed arguments that the ISU lacks sector-specific expertise, and lauded its efforts to consult with other government agencies. It therefore appears likely that the ISU will continue to seek the views of other UK Government departments in future NSIA reviews. Moreover, the Court set a high bar of deference despite various mitigation measures offered by LetterOne as an alternative to outright divestment, including restrictions on data flows (including personal information) between Upp and LetterOne, restrictions on physical and virtual access to Upp's sites, data and personnel by certain LetterOne representatives, and limitations on Board appointees. The judgment suggests that companies may have a larger hurdle to overcome than proposing contractual measures, standing alone, to mitigate national security risk. Even though the High Court conceded that, in light of those measures, the risk of interference by the Russian state was at a "near vanishing point,"

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

they did not suffice as other types of intervention, such as deceit, manipulation, or other forms of pressure, could still be applied. Despite presenting avenues of possible recourse to LetterOne, the High Court offered little sympathy, noting that losing money on investments that threaten national security is "ultimately part of the economic landscape." It will be interesting to see if this issue of financial compensation re-emerges in the current High Court appeal, as that body allowed financial compensation to be one of the bases on which permission to appeal was granted.

2. Outbound Investment

Finally, following speculation regarding the potential development of UK outbound investment controls, the UK Government amended its public guidance to clarify that the NSIA can apply to outward direct investment from the United Kingdom under certain circumstances. In particular, the NSIA potentially applies where a target entity outside the United Kingdom carries on activities in the United Kingdom or supplies goods or services to people in the United Kingdom, or where an asset being acquired from outside the United Kingdom is used in connection with activities in the United Kingdom or with the supply of goods or services to people in the United Kingdom. This guidance means that UK-based entities that acquire foreign entities or foreign assets, or that intend to enter into joint ventures with businesses that have no legal or physical presence in the United Kingdom, may nevertheless find their transactions subject to call in or, if relevant tests are met, mandatory notification. A sufficient connection to the United Kingdom includes, for example, research and development in the United Kingdom, an office located in the United Kingdom, or the supply of goods to a UK hub to send goods onward to other countries. Further, if an asset located outside the United Kingdom (including land, tangible moveable property, and intellectual property) is used by a party in the United Kingdom, by a party outside the United Kingdom to supply goods or services to the United Kingdom, or to generate energy or materials that are used in the United Kingdom, the asset is likely within the scope of the NSIA. Although the authority to review outbound investments is now theoretically available, it remains to be seen if and how these powers will be exercised by the UK Government, and how they will be balanced against the interests of the thriving UK investment community.

* * *

2024 was yet another extraordinarily active year in the world of trade controls. In light of President Trump's early actions to impose trade restrictions on allies and adversaries alike, and reprisals by leaders of major economies, we anticipate that with respect to sanctions, export controls, import restrictions, and foreign investment reviews, 2025 is unlikely to be quiet. Compliance-minded multinational enterprises should expect the unexpected, fasten their seatbelts, and prepare for turbulence ahead.

The following Gibson Dunn lawyers prepared this update: Scott Toussaint, Irene Polieri, Adam M. Smith, Stephenie Gosnell Handler, Christopher T. Timura, Ronald Kirk, Donald Harrison, Benno Schwarz, Michelle Kirschner, Attila Borsos, Samantha Sewall, Claire Shepherd, Alana Tinkler, Michelle Weinbaum, Roxana Akbari, Tina Asgharian, Grace Atkinson, Karsten Ball, Dharak Bhavsar, Sarah Burns, Alexa Bussmann, Soo-Min Chae, Martin Coombes, Justin duRivage, Hui Fang, Mason Gauch, Anna Helmer, Molly Heslop, Erika Suh Holmberg, Neringa Juodkunaite, Zach Kosbie, Josephine Kroneberger, Hayley Lawrence, Vanessa Ludwig, Nikita Malevanny, Jayee Malwankar, Nicole Martinez, Jacob McGee, Chris Mullen, Sarah Pongrace, Nick Rawlinson, Reed Sawyers, Anna Searcey, Alana Sheppard, Elsie Stone, Audi Syarief, and Lindsay Bernsen Wardlaw.

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.

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**

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) Donald Harrison – Washington, D.C. (+1
202.955.8560, dharrison@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) Amanda H. Neely – Washington, D.C. (+1
202.777.9566, aneely@gibsondunn.com) Samantha Sewall – Washington, D.C. (+1
202.887.3509, ssewall@gibsondunn.com) Michelle A. Weinbaum – Washington, D.C. (+1
202.955.8274, mweinbaum@gibsondunn.com) Hugh N. Danilack – Washington, D.C. (+1
202.777.9536, hdanilack@gibsondunn.com) Mason Gauch – Houston (+1
346.718.6723, mgauch@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) 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) Lindsay Bernsen Wardlaw – Washington,
D.C. (+1 202.777.9475, lwardlaw@gibsondunn.com) Shuo (Josh) Zhang – Washington,
D.C. (+1 202.955.8270, szhang@gibsondunn.com) **Asia**: Kelly Austin – Denver/Hong
Kong (+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) Arnold Pun – Hong Kong (+852 2214
3838, apun@gibsondunn.com) **Europe**: Attila Borsos – Brussels (+32 2 554 72
10, aborsos@gibsondunn.com) Patrick Doris – London (+44 207 071
4276, pdoris@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
224, nmalevanny@gibsondunn.com) Melina Kronester – Munich (+49 89 189 33
225, mkronester@gibsondunn.com) Vanessa Ludwig – Frankfurt (+49 69 247 411
531, vludwig@gibsondunn.com) © 2025 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com.
Attorney Advertising: These materials were prepared for general informational purposes only based on information available at the time of publication and are not intended as, do not constitute, and should not be relied upon as, legal advice or a legal opinion on any specific facts or circumstances. Gibson Dunn (and its affiliates, attorneys, and employees) shall not have any liability in connection with any use of these materials. The sharing of these materials does not establish an attorney-client relationship with the recipient and should not be relied upon as an alternative for advice from qualified counsel. Please note that facts and circumstances may vary, and prior results do not guarantee a similar outcome.

Related Capabilities

International Trade Advisory and Enforcement

© 2026 Gibson, Dunn & Crutcher LLP. All rights reserved. For contact and other information, please visit us at www.gibsondunn.com. | **www.gibsondunn.com**