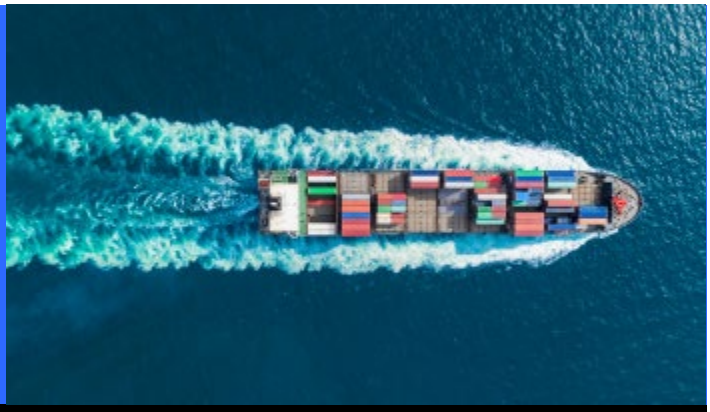
View on our website.

GIBSON DUNN



International Trade Advisory & Enforcement Update February 6, 2026

International Trade 2025 Year-End Update

The Trump administration re-entered the White House with an expansive vision for how international trade tools can be wielded to meet a range of "America First" policy goals. After one year in office, we have seen an unprecedented deployment of old and new tools of economic coercion wielded against allies and adversaries alike—with countermeasures wielded by them in response. Businesses, governments, and consumers throughout the world have found themselves on the front lines of this tit-for-tat throughout 2025, experiencing significant uncertainties and challenges that will only increase in 2026.

Upon his return to the White House in January 2025, President Trump quickly promulgated "America First" Trade and Investment Policies, laying out roadmaps for the administration's priorities and methodologies to achieve its strategic objectives. One year into the administration, it is clear that implementation of these policies has pushed economic statecraft to new, untested limits.

Certain cornerstones of U.S. trade policy have carried over with the new administration, including robust imposition and enforcement of sanctions and export controls and the policy stance that the United States is open for foreign investment. However, the first year of the second Trump administration has been set apart by the dominance of an additional tool of economic coercion—the unprecedented use of tariffs, including (even more innovatively) the newly emerged "secondary tariff." Deployed as a negotiating tool against strategic rivals and core partners alike, tariffs have emerged as the administration's favored tool to achieve foreign policy, national security, and domestic economic objectives. The novel imposition of tariffs pursuant to the International Emergency Economic Powers Act of 1977, a decades-old statute that underpins the vast majority of U.S. sanctions and other trade-related initiatives such as outbound investment

regulations, has further pushed the limits of U.S. law—so much so that the U.S. Supreme Court is set to weigh in on their legality in the coming weeks or months.

As Washington initiated fundamental shifts and policy reorientations, the European Union and the United Kingdom continued to build on the groundwork they have been laying over the last few years, cementing trade controls as strategic pillars of their foreign policies rather than solely reactive measures or follow-on tools to what the United States may impose. The EU Member States' increased alignment of sanctions violations penalties and the United Kingdom's establishment of a new sanctions enforcement body enhance enforcement risk for multinational firms that have until now primarily had to contend with U.S. enforcement agencies.

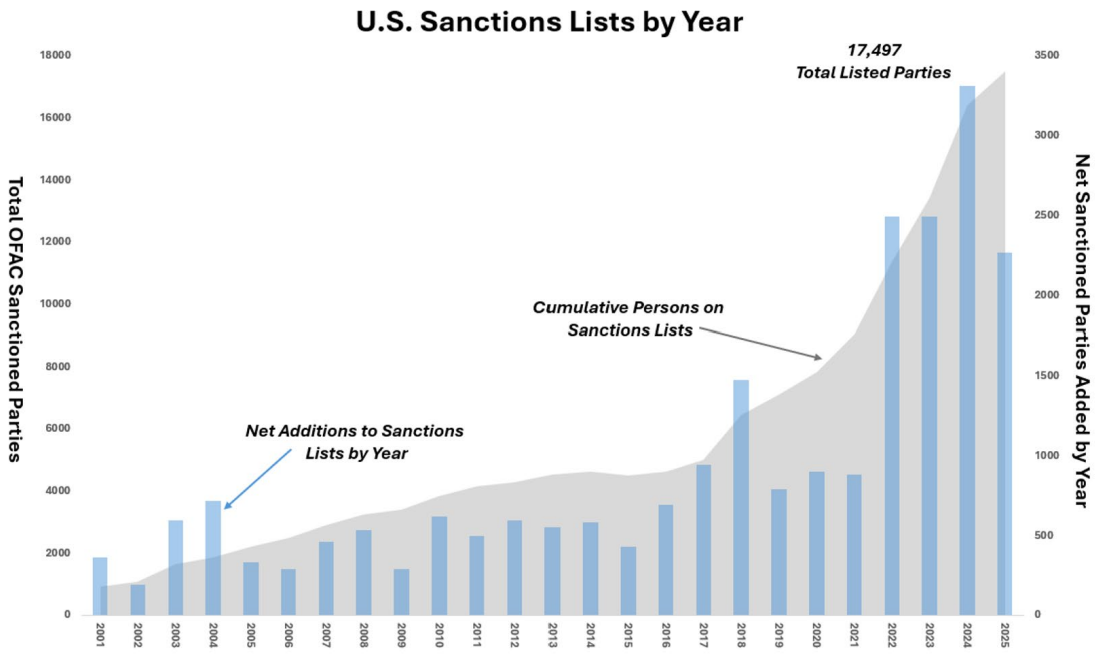
The United States and its traditional allies have undoubtedly experienced friction in connection with evolving policy approaches throughout 2025. However, the year also showed important signs of continued collaboration amidst common goals and strategic priorities. The snapback of EU and UK sanctions on Iran brought those sanctions regimes into closer alignment with the United States, which continued to ramp up pressure on Iran—the primary focus of new U.S. sanctions designations in 2025. Coordinated EU, UK, and U.S. sanctions targeting Russia's largest oil producers struck at the core of Russia's hard currency revenue streams, as efforts to broker peace between Moscow and Kyiv stalled. This alignment even extended to the lifting of sanctions, as all three jurisdictions moved to ease long-standing restrictions on Syria after the Assad regime was deposed and new leadership emerged.

Still, as renewed threats of tariffs dominated the news cycle in the early weeks of 2026, "America First" is poised to continue driving the Trump administration's approach to trade controls in the coming years, with immediate and long term consequences for allies and geostrategic competitors. As a result, the increased uncertainty that characterized 2025 is unlikely to subside in the year ahead.

TABLE OF CONTENTS

I. U.S. SANCTIONS

The total number of U.S. sanctioned parties continued to climb in 2025. As always, however, the numbers only tell part of the story.



Iran supplanted Russia as the chief target of new list-based U.S. sanctions, accounting for around half of all designations by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) in 2025. While the year reflected a substantial number of new sanctions designations, hundreds of parties in Syria were also *de*-listed as the Trump administration lifted a comprehensive embargo to give breathing room to the new Syrian government.

And in stark contrast to the Biden administration, the Trump administration's deployment of economic tools was often prelude to its deployment of military tools. The reimposition of "maximum pressure" on Iran in the first days of the new Trump administration, including a relentless series of sanctions on Tehran's revenue sources and defense networks, escalated by mid-year into U.S. airstrikes targeting Iranian nuclear facilities. Unprecedented designations of cartels and drug trafficking groups as terrorist organizations foreshadowed U.S. military strikes on alleged drug smuggling boats in the Caribbean. A tightening of sanctions targeting Venezuela's energy sector was followed by oil tanker seizures and, at the start of 2026, a stunning U.S. military operation in Caracas to capture Venezuelan President Nicolás Maduro.

A. Iran

Relations between the United States and Iran entered a volatile phase during 2025 as President Trump, within days of re-entering the Oval Office, announced the resumption of his first term's "maximum pressure" campaign against Tehran. In a bid to deny Iran a nuclear weapon, halt its ballistic missile program, and disrupt its destabilizing activities abroad, the new U.S. administration accelerated the pace of Iran sanctions designations, pressed the regime to return to the negotiating table, and, in June, launched an airstrike against three Iranian nuclear facilities.

The Islamic Republic—alongside a small handful of other jurisdictions, including Cuba, 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 almost any dealings involving Iran. In addition to those restrictions, during 2025 OFAC added to its Specially Designated Nationals and Blocked Persons (SDN) List nearly one thousand individuals, entities, vessels, and aircraft tied to high-priority sectors of the Iranian economy. Frequent targets of Iran-related sanctions designations included parties allegedly involved in:

- The Iranian petroleum and petrochemicals trade, with a particular focus on shippers and vessels comprising the Iranian "shadow fleet," along with China-based importers and refiners of Iranian crude;
- The Iranian shadow banking system, including parties using neighboring states such as the United Arab Emirates as sanctions evasion and transshipment hubs; and
- The Iranian defense sector, including nuclear, ballistic missile, and unmanned aerial vehicle (UAV) procurement networks.

The United States was not alone in pressuring Iran. The U.S. attack on Iranian nuclear targets took place alongside Israel's 12-day war in June 2025, which battered the Islamic Republic's air defenses and domestic political standing. Iran's economic and diplomatic isolation further deepened in September 2025 with the snapback of UN, EU, and UK sanctions (discussed further below) that for the past decade had been suspended under the Joint Comprehensive Plan of Action (JCPOA)—commonly known as the Iran nuclear deal. By early 2026, Tehran found itself mired in a deepening currency crisis, roiled by anti-government demonstrations, and bracing for possible U.S. military action as the regime brutally cracked down on protesters.

Barring further dramatic developments on the ground, the Trump administration appears set to continue prosecuting its maximum pressure campaign throughout the near future. In light of the President's stated objective of driving Iranian oil exports to zero, further sanctions designations targeting shipping companies, vessels, oil traders, and financial institutions dealing in Iranian barrels are likely on the horizon. As seen in Venezuela, it is possible that the Trump administration may take to boarding and seizing vessels carrying Iranian crude. It is also conceivable that the Trump administration could in coming months begin targeting larger, more economically consequential parties based in the People's Republic of China (PRC)—by far the largest remaining buyer of Iranian crude—though at the risk of upsetting the fragile trade truce between Washington and Beijing.

B. Russia

Following a three-year period in which the United States, in concert with its allies and partners, imposed historic trade restrictions on Russia, the pace of new U.S. sanctions targeting Russia slowed in 2025 as President Trump sought to broker peace between Moscow and Kyiv. When talks failed to end the fighting in Ukraine, the United States intensified pressure on Russia's crucial energy sector, including by increasing tariffs on a key buyer of Russian crude, blacklisting two Russian oil majors, and threatening sharply higher duties on countries that import Russian energy.

Similar to the strategy adopted by the prior U.S. administration as it worked to coax Iran to resume nuclear negotiations, President Trump unveiled no new sanctions on Russia during his first six months in office in a seeming effort to create space for peace talks to progress. However, the Trump administration's patience with Moscow appeared to wear thin in August 2025 when, on the eve of a major summit between Presidents Trump and Putin, the White House announced unprecedented "secondary tariffs" on India stemming from Delhi's continued purchases of Russian oil. From a policy perspective, that novel measure—which involves levying increased duties on *all* Indian-origin goods entering the United States, rather than penalizing specific firms involved in the Russian oil trade—appears calculated to limit the Kremlin's ability to finance its war effort by deterring foreign governments from allowing Russian petroleum and petroleum products into their territories. As part of a reported U.S.–India trade deal, President Trump indicated in early February 2026 that the United States had agreed to reduce tariffs on India, which will in turn stop buying Russian oil. The effectiveness of these measures in halting the war in Ukraine will likely hinge on whether the Trump administration is prepared to impose similar restrictions on China, the world's most prolific consumer of Russian oil.

As peace negotiations dragged on, President Trump in October 2025 ratcheted up pressure on Russia's energy sector by imposing full blocking sanctions on the country's two largest oil producers, ***Rosneft*** and ***Lukoil***. 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 "50 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 on the list.

Although the U.S. government targeted relatively few Russia-related parties this past year—together representing a tiny percentage of new OFAC sanctions designations announced during 2025—Rosneft and Lukoil are among the largest and most economically consequential enterprises ever subjected to a U.S. asset freeze. The impact of those designations on the global oil market was further magnified by similar measures from the European Union and the United Kingdom (discussed further below). The joint designations represented a fundamental shift in U.S., EU, and UK thinking on Moscow. Ever since the Crimean invasion in 2014, the Western powers have carefully avoided blacklisting large parts of the Russian energy sector for fear of upsetting global markets and denying European and Japanese allies critical fuels they came to rely upon Russia to provide. No more. That the European Union followed this designation with a pronouncement that the bloc will be free of Russian oil purchases by 2027 underlined the rupture between Russia and what had been its principal markets.

President Trump, at least in the near term, appears set to maintain and potentially expand U.S. sanctions on Russian energy to maximize U.S. leverage in negotiations with Moscow. One option available to the administration to increase pressure on the Kremlin could involve urging

the U.S. Congress to adopt the Sanctioning Russia Act—a bill spearheaded by Senators Lindsey Graham (R-SC) and Richard Blumenthal (D-CT) that enjoys bipartisan support on Capitol Hill and would authorize "bone crushing" secondary tariffs of up to 500 percent on all goods imported into the United States from any country that knowingly purchases Russian-origin oil, petroleum products, or uranium. It is also possible that the White House could threaten to impose "secondary sanctions" (i.e., penalties up to and including blocking use of the U.S. financial system or freezing all property interests) on foreign financial institutions that continue to process payments involving Russian petroleum and petroleum products. This would be an add-on to the Biden-era authority that threatens to impose secondary sanctions on foreign banks that process transactions involving Russia's military-industrial base.

Conversely, if talks among Washington, Moscow, and Kyiv bear fruit, it would not be surprising if the White House were to quickly ease restrictions on dealings involving Russia. With the narrow exception of certain U.S. sanctions designations pursuant to Executive Order 13662, nearly all Biden- and Trump-era measures targeting Russia (which were implemented via Executive Order) can be 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 Executive Order 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, especially in light of the perceived broader threat that Russia poses to select EU Member States.

C. Syria

One of the most unexpected and consequential trade developments of 2025 involved the United States' easing of sanctions on Syria. This policy change, announced by President Trump to the surprise of most observers while on a state visit to Saudi Arabia in May 2025, involved the White House quickly paring back most U.S. trade restrictions—including lifting comprehensive sanctions on Syria—as it sought to bolster the government of President Ahmed al-Sharaa and facilitate the country's reconstruction. Although the continuing rapprochement between Washington and Damascus suggests that remaining restrictions could be eased in coming months, the new government still faces significant challenges in consolidating power, and it will take time for policymakers to disassemble the full suite of U.S. trade controls on Syria, some of which require an act of Congress to revoke.

In its first moves to unwind Syria restrictions, the United States in early 2025 issued two general licenses authorizing a steadily broader range of transactions involving Syria. The first such license, issued in January 2025, permitted U.S. persons to engage in certain limited transactions involving Syria's post-Assad governing institutions, the country's energy sector, and the processing of noncommercial, personal remittances. In May 2025, OFAC—in a move that foreshadowed more lasting sanctions relief to come—issued a separate general license authorizing U.S. persons to engage in substantially all transactions prohibited by the agency's Syrian Sanctions Regulations, including making new investments in Syria, exporting services to Syria, and importing into the United States Syrian-origin petroleum or petroleum products.

Concurrent with that May 2025 announcement, the U.S. Department of State issued a 180-day waiver of certain provisions of the Caesar Syria Civilian Protection Act of 2019 (the Caesar Act)—a statute that then mandated sanctions against non-U.S. persons that knowingly engage in certain significant transactions involving Syria—in a bid to reassure humanitarian aid organizations and prospective foreign investors considering re-entering the Syrian market.

As described in a prior client alert, President Trump in June 2025 built on those measures by issuing a groundbreaking Executive Order that replaces longstanding comprehensive sanctions on Syria with a targeted, list-based sanctions program that restricts dealings involving certain specified bad actors such as terrorist organizations and Assad regime insiders. Among other key changes, that order revoked the Syrian Sanctions Regulations, enabled the lifting of blocking sanctions on over 500 Syria-related parties, and allowed the U.S. Department of Commerce's Bureau of Industry and Security (BIS) to waive certain export controls, while the State Department set in motion a process to eventually rescind Syria's designation as a State Sponsor of Terrorism (SST).

The United States continued to peel back layers of restrictions on Syria as 2025 wound down. The Commerce Department issued a final rule that, as of September 2025, authorizes exports to Syria of EAR99 items (i.e., goods, software, and technology that have purely civilian uses) to most end users under a new License Exception Syria Peace and Prosperity (SPP). In November 2025, the State Department lifted blocking sanctions on President al-Sharaa—until then, a designated terrorist—ahead of a White House summit with President Trump. Finally, in an apparent effort to provide more certainty for non-U.S. parties, Congress in December 2025 repealed the Caesar Act and its mandatory secondary sanctions, thereby eliminating a major deterrent to the large-scale, long-term capital investments that Syria will need to rebuild its shattered economy after a more than decade-long civil war.

Despite considerable U.S. sanctions relief over the past year, not all U.S. trade restrictions on Syria have been lifted. For example, Syria remains home to several hundred individuals and entities that are subject to U.S. blocking sanctions by virtue of appearing on OFAC's SDN List. Syria also remains subject to a trade embargo under the U.S. Export Administration Regulations (EAR) as well as an arms embargo under the U.S. International Traffic in Arms Regulations (ITAR), and the country continues to be designated an SST, with the result that U.S. foreign assistance and certain U.S. exports to Syria are restricted.

While more regulatory changes will be needed to prove that the new Syria is truly "open for business," post-Assad Syria has been granted a meaningful opportunity to re-enter the global economy. In recent weeks, however, the Syrian government has made advances to reclaim control over large areas of territory in eastern and northern Syria, testing U.S. support of the new government as it has clashed with the Kurdish-led Syrian Democratic Forces that have been a key U.S. partner in the fight against the Islamic State. The further easing of U.S. restrictions targeting Syria may well hinge on how President al-Sharaa handles this and other challenges in coming months as he continues his efforts to unite his fractured nation.

D. Venezuela

Although traditional U.S. trade controls on Venezuela were largely quiet for much of the past year, sanctions tell only part of the story. President Trump during 2025 renewed his first term's hardline focus on the regime of President Nicolás Maduro, including by massing forces in the Caribbean, striking alleged drug-trafficking vessels, partially blockading Venezuela's coast, seizing tankers carrying Venezuelan oil, and in early January 2026 launching a midnight raid that resulted in Maduro's capture and extradition to the United States. As of this writing, Maduro's top lieutenants remain in charge in Caracas and U.S. sanctions are mostly unchanged—though restrictions on Venezuela's crucial oil sector have already been eased as the Trump administration looks to stem the flow of migrants and jumpstart Venezuela's moribund economy.

U.S. sanctions on Venezuelan energy seesawed during the first half of 2025. Starting in March 2025, OFAC replaced a longstanding general license, which authorized certain transactions related to the operation and management by a U.S. energy company of its joint ventures involving the state-owned oil giant ***Petróleos de Venezuela, S.A.*** (PdVSA), with a series of time-limited wind-down authorizations. The Trump administration allowed that license, along with a separate general license that permitted certain Venezuela-related dealings involving four named U.S. oilfield services companies, to expire in May 2025. According to news reports, the White House quietly reversed course in July 2025 by issuing one or more OFAC specific licenses authorizing the U.S. energy company at issue to resume many of its prior activities in Venezuela, including the exportation to the United States of Venezuelan-origin oil.

President Trump in parallel moved to deter shipments of Venezuelan oil to other jurisdictions, including by issuing an Executive Order in March 2025 authorizing secondary tariffs on all goods imported into the United States from any country determined by the U.S. Secretary of State to have imported Venezuelan-origin petroleum or petroleum products on or after a certain date. Unlike in the Russia context, the Trump administration has not yet levied any such duties. Indeed, in light of the apparent U.S. policy interest in reviving Venezuelan energy production following President Maduro's January 2026 ouster, the threatened Venezuela-related tariffs seem unlikely to be implemented by the Trump administration, at least in the near term. Rather, an Executive Order signed by President Trump in late January 2026 authorizing secondary tariffs on any country determined to sell oil to Cuba may reflect a new approach by the administration in pursuit of its Western Hemisphere policy objectives.

As we observed in a prior client alert, although President Maduro has been removed from office, power in Caracas has not changed hands, and U.S. trade restrictions broadly remain the same. U.S. persons continue to be, except as authorized by OFAC, prohibited from engaging in transactions involving the Government of Venezuela, which is defined to include not just government agencies and political subdivisions, but also any entity that is majority-owned or controlled by the government. Consequently, U.S. persons (and non-U.S. persons when engaging in a transaction with a U.S. touchpoint) potentially risk triggering U.S. sanctions when dealing with an arm of the Venezuelan state, such as a state-owned enterprise like PdVSA or the country's central bank. Over 400 parties, including public and private firms, presently appear on the SDN List pursuant to various Venezuela-related legal authorities.

The situation on the ground in Venezuela remains highly fluid. As U.S. sanctions targeting the Maduro regime are not codified in statute, they can be quickly eased through executive action—including, for example, issuing (or re-issuing) OFAC general licenses authorizing certain dealings involving the country's energy sector, de-listing PdVSA, or conceivably lifting blocking sanctions on the entirety of the Government of Venezuela. As an initial step, the Trump administration announced plans to "selectively roll[] back sanctions to enable the transport and sale of Venezuelan crude and oil products to global markets." Executive Order 14373 quickly followed, creating an untested mechanism for U.S. government oversight of certain Venezuelan oil revenues. OFAC in late January 2026 further paved the way for Venezuelan crude to be sold on legitimate global markets with the issuance of Venezuela General License 46, authorizing, subject to certain conditions, established U.S. firms to engage in transactions that are "ordinarily incident and necessary to the lifting, exportation, reexportation, sale, resale, supply, storage, marketing, purchase, delivery, or transportation of Venezuelan-origin oil, including the refining of such oil."

A further easing of U.S. restrictions could be contingent upon the leadership in Caracas meeting certain milestones, such as curbing illicit drug trafficking and irregular migration, distancing itself from Cuba, Iran, China, and Russia, and perhaps taking concrete steps toward the restoration of Venezuelan democracy.

E. Counter-Terrorism and Counter-Narcotics

In addition to measures targeting countries such as Iran and Russia, the United States in 2025 vigorously used OFAC's thematic sanctions programs, which are global in nature and seek to deter particular types of conduct such as human rights abuses or corruption no matter where they occur. In one of the signature trade developments of the past year, the Trump administration often wielded counter-terrorism and counter-narcotics sanctions authorities against novel targets, including drug cartels, organized crime groups, and sitting heads of state.

Following an election campaign in which he declared illegal immigration, violent crime, and drug trafficking to be core national priorities, on Inauguration Day, President Trump signed an Executive Order declaring it the policy of the United States to ensure the "total elimination" of cartels and transnational criminal organizations—and setting in motion a process to name such groups Specially Designated Global Terrorists (SDGTs) and Foreign Terrorist Organizations (FTOs). During 2025, the Trump administration applied the more restrictive FTO label—which can trigger criminal, civil, and reputational consequences for parties that engage with such organizations—to a record-shattering 25 new entities. Such counter-terrorism designations (or, in many cases, re-designations) targeted major Mexican drug cartels and South American criminal enterprises such as Tren de Aragua, as well as Yemen's Ansarallah (commonly known as the Houthis) and several European anti-fascist groups.

SDGT and FTO designations are similar in that each involves the imposition of U.S. blocking sanctions. Upon becoming designated an SDGT, an FTO, 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 and U.S. persons are, except as authorized by OFAC, generally prohibited from engaging in transactions involving the blocked person and their majority-owned entities.

The chief difference between those two types of counter-terrorism designations is that being named an FTO triggers further, onerous restrictions that are unique among U.S. sanctions programs. In particular, designation as an FTO results in the targeted organization becoming blocked and *also* (1) renders representatives and members of the FTO, if they are not U.S. citizens or U.S. nationals, inadmissible to the United States; (2) exposes persons subject to U.S. jurisdiction to criminal liability for knowingly providing "material support or resources" to the FTO; and (3) gives rise to a private right of action in which terrorism victims can bring civil suits against, and seek treble damages from, parties that knowingly provide "substantial assistance" to an FTO. Certain dealings with SDGTs (a list which, as of today, also includes all FTOs) can further trigger U.S. Securities and Exchange Commission reporting obligations.

Historically, U.S. counter-terrorism sanctions (and their attendant consequences) have been reserved mostly for Islamist militant groups based in the Middle East and South Asia, such as al-Qaeda and ISIS. The Trump administration's unprecedented use of counter-terrorism authorities to target apolitical, profit-driven groups based in the Western Hemisphere presents substantial practical challenges for enterprises operating in Latin America. For example, Mexico-based cartels are tightly integrated into the legitimate economy of a major U.S. trading partner and seldom appear by name on invoices or other transaction documentation. Moreover, in light of the lower threshold for criminal liability and the possibility that a U.S. court could award substantial monetary damages, FTO designations can result in de-risking by financial institutions and other key business partners that may be prohibited from (or otherwise unwilling to engage in) transactions that could, directly or indirectly, involve such a named terrorist group. Accordingly, it is prudent for businesses with activities in Latin America and the Caribbean to conduct restricted party screening and enhanced due diligence to assess whether their current or prospective counterparties have links to newly designated terrorist organizations.

In tandem with counter-terrorism measures, the Trump administration has increasingly used U.S. counter-narcotics sanctions as a cudgel against left-leaning political figures in South America. Notably, the United States on multiple occasions this past year imposed sanctions on the Cartel de los Soles, purportedly led by Venezuela's President Nicolás Maduro. In October 2025, the U.S. government, in a surprise action against a longstanding security partner and a Major Non-NATO Ally, designated the President of Colombia pursuant to a counter-narcotics authority following his vocal criticism of U.S. airstrikes off the Venezuelan coast.

In coming months, the Trump administration appears set to continue heavily using terrorism- and narcotics-related sanctions to advance the White House's domestic policy priorities and discredit opponents abroad, even at the expense of dulling the moral sting that has traditionally accompanied the use of such tools.

F. International Criminal Court

The White House extended its aggressive use of OFAC's thematic authorities by reviving a short-lived and unorthodox sanctions program—created under the first Trump administration and quickly dismantled by President Biden—targeting certain parties associated with the International Criminal Court (ICC).

In February 2025, President Trump issued an Executive Order resuscitating the ICC sanctions program, citing that body's threat to the sovereignty of states, such as the United States and Israel, that are not party to the Rome Statute and have not consented to the ICC's jurisdiction. Concurrent with that order, the United States imposed blocking sanctions on the court's chief prosecutor, stemming from his involvement in the issuance of an arrest warrant against Israel's Prime Minister Benjamin Netanyahu and former Defense Minister Yoav Gallant. As a result of further designations announced in June, July, August, September, and December 2025, the United States has added to the SDN List a total of 15 parties associated with the court, including specific judges, prosecutors, and nongovernmental organizations deemed to be supporting ICC investigations of Israeli nationals.

U.S. sanctions targeting the ICC are presently limited in scope. Although U.S. persons are restricted from engaging in transactions involving the 15 named parties associated with the ICC who appear on the SDN List (as well as those parties' majority-owned entities), OFAC has indicated in various contexts that, as a general matter, "when a designated individual has a leadership role in a governing institution, the governing institution is not itself considered blocked." Consequently, absent the involvement of a sanctioned party, U.S. persons are *not* generally restricted by OFAC sanctions from engaging in activities involving the ICC as an institution or its various organs, such as the Office of the Prosecutor, the Presidency, or the Judicial Divisions.

The return of U.S. sanctions targeting ICC personnel, including lawyers and jurists, highlights the Trump administration's willingness to impose sanctions against non-traditional targets and without coordination with, or support from, traditional U.S. allies. This trend was reinforced by the July 2025 sanctions targeting Brazilian Supreme Federal Court Justice Alexandre de Moraes, one of only a few designations this year under OFAC's human rights-focused Global Magnitsky sanctions (although Justice Moraes was removed from the SDN List by year's end). If in the future the ICC were to launch an investigation into conduct by President Trump, other senior U.S. officials, or U.S. military personnel, it is possible that the United States could expand its existing sanctions to prohibit U.S. nexus dealings involving the ICC itself. Any such expansion is likely to be met with U.S. legal challenges, as certain U.S. district courts have already expressed skepticism of the legality of the current ICC sanctions on First Amendment grounds, at least as applied to certain U.S. citizens supporting the court's activities.

G. Enforcement Trends

1. OFAC Enforcement Actions and Compliance Lessons

2025 was a busy year for OFAC enforcement as the agency, across 14 enforcement actions, imposed a combined $265.7 million in fines—a fivefold increase over the prior year. That uptick was principally driven by a blockbuster $215.9 million penalty against a California venture capital firm stemming from alleged dealings involving a sanctioned Russian oligarch. But for that case, the aggregate amount of fines levied by OFAC would have been roughly on par with the agency's five-year median of approximately $50 million in civil monetary penalties per year.

Notably, 8 of the 14 OFAC enforcement actions announced during 2025—including the five largest resolutions of the year—involved apparent Russia sanctions violations. While

enforcement actions are often a trailing indicator of OFAC enforcement priorities, as matters can take several years to resolve after a potential violation has been identified, this trend nonetheless suggests that dealings involving the Russian Federation—and, in particular, Russian oligarchs—is likely to remain an area of continued enforcement for U.S. authorities in coming months.

We highlight below the most noteworthy compliance lessons from OFAC's 2025 enforcement activity. Many of these takeaways were explicitly communicated by OFAC through the "compliance considerations" section included in the web notice for each of its enforcement actions:

- **"Gatekeepers" can be subject to heightened sanctions compliance expectations**: The role of gatekeepers—sophisticated U.S. parties such as investment advisors, accountants, attorneys, trust and corporate formation service providers, and real estate professionals—was a major theme of OFAC's enforcement activity this past year. OFAC repeatedly emphasized that such individuals occupy positions of trust, have considerable access to information, and can lend a transaction involving a sanctioned party an air of legitimacy. Consequently, such professionals may be subject to heightened expectations to monitor for and detect potential sanctions evasion, and should conduct thorough due diligence into prospective clients to minimize the risk of their services facilitating a restricted party's access to the U.S. financial system.

- **Transaction parties should be alert to indications that a sanctioned party owns—or controls—property**: Several of OFAC's recent cases highlight the importance of understanding potential sanctioned-person control or influence over investments—even when such persons are not named in transaction documentation such as deeds, property records, or contracts. Professionals and professional services firms should be sensitive to the possibility that blocked persons may be indirectly involved in a transaction, including through proxies or opaque legal structures. OFAC has further cautioned that transaction parties and their advisors should avoid formalistic analyses and, where appropriate, look beyond nominal ownership to a transaction's underlying practical and economic realities—a trend that puts considerable pressure on OFAC's ownership-driven 50 Percent Rule and suggests that over time OFAC may move to an "ownership or control" test with respect to downstream sanctions impacts like that in place in the European Union and the United Kingdom.

- **Transaction parties should heed OFAC blocking notifications and cease-and-desist orders**: OFAC enforcement activity suggests that the agency is increasingly using notifications of blocking and cease-and-desist orders to alert interested parties to the existence of a blockable property interest before a sanctions violation (or further violation) occurs. Such notices can also be used by OFAC to show that a party had actual knowledge that a subsequent transaction involving that property might implicate the agency's prohibitions. In at least two enforcement actions published in 2025, transaction parties appear to have disregarded such explicit warnings. Recipients of blocking notifications and cease-and-desist orders should take such notices seriously, closely scrutinize the person or property identified by the agency, and timely block and report to OFAC any property within U.S. jurisdiction in which a blocked person holds an interest.

- **OFAC may be less willing to settle**: Historically, the vast majority of OFAC enforcement actions resulting in monetary penalties were resolved with a settlement agreement. The issuance of a penalty notice—a mechanism by which OFAC unilaterally announces its determination that a violation of its regulations has occurred and imposes a penalty in whatever amount it deems appropriate—has been rare. In a departure from past practice, OFAC in 2025 resolved three cases, each involving a Russian oligarch and

conduct that the agency deemed egregious, by issuing a penalty notice to the alleged violator in lieu of settling. Such resolutions, which have in the past often triggered a lawsuit by the enforcement target, appear calculated to convey to the regulated community that there are certain cases about which OFAC feels especially strongly and is prepared to litigate if necessary.

- **OFAC is increasingly holding individuals accountable for U.S. sanctions violations**: OFAC this past year imposed substantial civil monetary penalties against three unnamed individuals for providing professional services to blocked persons, breaking from the agency's recent practice of levying fines almost exclusively against corporate entities. Indeed, prior to 2025, OFAC had penalized only five natural persons during the preceding ten years combined. The agency's recent enforcement activity suggests that individual professional service providers should familiarize themselves with common "red flags" for sanctions risk, understand how their work could expose them to sanctions liability, and conduct careful due diligence on higher-risk clients.

2. U.S. Department of Justice Enforcement Priorities

Alongside robust civil enforcement by OFAC, the U.S. Department of Justice (DOJ) announced in May 2025 that it would prioritize criminal enforcement of sanctions evasion. In a memorandum detailing its new White Collar Enforcement Plan, DOJ's Criminal Division directed its prosecutors to focus on, among other top priorities, national security offenses, including pursuing "gatekeepers, such as financial institutions and their insiders that commit sanctions violations or enable transactions" by drug cartels, transnational criminal organizations, hostile nation-states, and FTOs. As we described in a prior client alert, the memorandum also calls for an "America First," business-friendly approach to white collar enforcement, which could ultimately lead to fewer or less aggressive prosecutions of U.S. companies. In light of the memorandum's explicit focus on sanctions evasion as both a criminal and national security concern, we anticipate that DOJ, including not just the Criminal and National Security Divisions in Washington, but also individual U.S. Attorney's offices around the country, will vigorously pursue financial institutions that facilitate sanctions evasion by processing illicit transactions.

In line with DOJ and OFAC efforts to combat sanctions evasion, U.S. authorities this past year continued to engage in a multi-agency push to both prosecute and sanction parties involved in North Korea's sustained effort to generate hard currency to fund North Korea's weapons of mass destruction programs, through the placement of remote information technology (IT) workers across hundreds of U.S. companies. As part of this IT worker scheme, which has been active for several years, a sizeable contingent of North Korean individuals have fraudulently obtained remote employment with U.S.-based companies, leveraging stolen identities of U.S. persons, and relying on the assistance of U.S.-based individuals. While the primary objective of the scheme appears to be to raise currency for the North Korean regime, the scheme—which sees remote IT workers performing routine tasks in corporate roles such as software development—also enables access by these remote workers to potentially sensitive data, including source code and export-controlled data. There have been reports of data exfiltration and extortion in connection with this scheme, in addition to collection of salaries.

In June 2025, DOJ announced nation-wide, coordinated law enforcement actions against the North Korean IT worker scheme, resulting in the indictment of 13 individuals (including two U.S. nationals, who have both pleaded guilty), and the seizure of 29 financial accounts and approximately 200 laptops used to facilitate remote access to U.S. company systems. The next month, in July 2025, an Arizona woman was sentenced to 8.5 years in prison for her role in helping North Korean IT workers obtain jobs at over 300 U.S. companies. And in November 2025, DOJ announced five further IT worker-related guilty pleas and over $15 million in civil forfeiture actions. OFAC complemented DOJ's efforts on multiple occasions designating non-U.S. parties implicated in the scheme. In light of North Korea's decades-long isolation from the mainstream global economy, further attempts to penetrate U.S. businesses, along with associated prosecutions and sanctions designations, are likely to persist in the months ahead. Although the U.S. government has so far been treating victim companies as partners in these enforcement efforts, businesses reliant on remote IT workers are on notice of the red flags consistent with the scheme and should ensure appropriate diligence throughout hiring and employment processes to mitigate risk.

II. U.S. EXPORT CONTROLS

U.S. export controls have further cemented their place alongside sanctions as key tools in furthering U.S. national security and foreign policy objectives, particularly as the United States seeks to restrict access to certain advanced technologies by perceived geopolitical competitors like China. Yet, the role of export controls in 2025 has been complicated by political tides that ushered in significant institutional changes at the U.S. Department of Commerce's Bureau of Industry and Security, the agency primarily responsible for administration of U.S. export controls on goods, software, and technology that have both military and civilian uses (commonly known as "dual-use" items).

A number of longtime BIS officials departed the agency, known for its technically complex regulations, which has led to a lull in new rules and a spike in export licensing wait times. At the same time, the second Trump administration has increasingly reached for export controls as a bargaining chip at the diplomatic negotiating table, both with China and with U.S. industry. The result was a year of starts and stops, where landmark new rules were paused or walked back not long after they were announced, creating uncertainty among industry about compliance expectations.

Despite these institutional challenges, export enforcement showed no signs of slowing down. With significant enforcement actions from both BIS and DOJ, the new administration seemed to follow through on Commerce Secretary Howard Lutnick's assurances during his confirmation hearings that aggressive export enforcement would be a priority. As BIS has now received a 23 percent funding increase from Congress for fiscal year 2026, continued robust enforcement is expected, even if the longer-term impact of personnel turnover remains to be seen.

A. Artificial Intelligence

1. AI Diffusion Rule Rescission and Shift in Semiconductor Export Control Strategy

In its closing days, the Biden administration issued the Artificial Intelligence (AI) Diffusion Rule, a sweeping interim final rule to control access to advanced AI capabilities by establishing chokepoints over three key exports: advanced integrated circuits (ICs); compute power; and model weights. On May 13, 2025, two days before the AI Diffusion Rule's effective date, the Trump administration announced its rescission of the rule, citing concerns that its burdensome regulatory requirements could undermine innovation and that its tiered licensing system could generate adverse diplomatic consequences.

The policy shift is consistent with a broader trend in U.S. export control strategy toward pairing restrictive measures with affirmative efforts to shape global technology ecosystems around U.S. supply chains, standards, and compliance expectations—particularly in strategically significant regions such as the Middle East. China's continued development of advanced AI models despite extensive U.S. export controls appears to have informed this approach. Against this backdrop, the rescission of the AI Diffusion Rule—together with approvals conditionally permitting additional exports of advanced semiconductors to the United Arab Emirates and a series of AI initiatives involving the United Arab Emirates and Saudi Arabia—reflects an effort to expand the reach of U.S.-aligned AI infrastructure and governance. Consistent with this trend, the White House's July 2025 AI Action Plan calls for the United States to "meet global demand for AI by exporting its full AI technology stack (hardware, models, software, applications, and standards) to all countries willing to join America's AI alliance." The plan was paired with a July 2025 Executive Order promoting the export of the American AI technology stack, which is in turn implemented through the October launch of the American AI Exports Program, though details of this program remain scant at present.

Despite the Trump administration's stated intent to replace the prior AI Diffusion Rule with a "stronger but simpler" framework, BIS has not yet issued replacement regulations. And although BIS recently loosened restrictions on the export of certain advanced chips to China, the manufacturing equipment used to build them and most AI-capable hardware remain subject to significant licensing constraints. As discussed in a prior client alert, we believe that any replacement framework is likely to retain core elements of the rescinded rule, including differentiated treatment for trusted jurisdictions, some form of validated end-user or equivalent authorization for data centers, enhanced customer diligence and reporting obligations, and controls on certain proprietary AI models. Indeed, many of these elements have been central parts of the Trump administration's partial lifting of controls on the UAE, Saudi Arabia, and China.

2. New Guidance Regarding Advanced Computing ICs

On the same day BIS announced the rescission of the AI Diffusion Rule, the agency issued new guidance underscoring its intent to continue tightening export controls targeting China. In particular, BIS invoked the Export Administration Regulations' expansive General Prohibition 10 (GP 10) to caution against transactions involving advanced Chinese ICs that meet or exceed the performance thresholds set forth in Export Control Classification Number (ECCN) 3A090. GP 10

generally prohibits dealings in items subject to the EAR where a known violation of the EAR has occurred, is about to occur, or is intended to occur in connection with the item.

According to BIS, due to the application of one or more foreign direct product rules—rules which bring within U.S. export control jurisdiction foreign-made items that incorporate, or are the direct product of, certain software and technology, or components made from U.S. inputs—there is a high likelihood that the design or production of certain advanced Chinese ICs involved violations of the EAR. As a result, BIS warned that dealings in such ICs, including through their purchase or use without authorization, could create enforcement risk. This guidance illustrates how GP 10 can extend export controls beyond export transactions to reach downstream commercial activity, including certain services and financial dealings.

BIS also issued a policy statement aimed at parties seeking to avoid hardware export controls by purchasing remote access to compute capacity, through Infrastructure-as-a-Service (IaaS) or GPU-as-a-Service arrangements, rather than acquiring such hardware directly. The policy statement indicates that a license requirement applies to the export, reexport, or transfer of advanced computing ICs, and commodities containing them, where the exporter has knowledge that they will be used to provide compute power for AI model training for or on behalf of a weapons of mass destruction or military-intelligence end users headquartered or operating in a country subject to a U.S. arms embargo (including China). BIS further indicated that U.S.-person support for such cloud-based activities may also require a license. While the contours of these restrictions have not yet been tested publicly through BIS enforcement actions, nor clarified through further guidance, they raise significant compliance considerations for cloud service providers, data center operators, and other participants in the AI infrastructure ecosystem.

Finally, BIS published accompanying red flags guidance identifying transactional and behavioral indicators of diversion risk and recommended enhanced due diligence measures for exporters of advanced computing ICs.

3. Revoked VEU Status for Certain Chipmakers in China

In the latter half of 2025, BIS revoked validated end-user (VEU) status—an authorization for pre-vetted end users to receive covered items without obtaining an otherwise-required license for each export—of several foreign-owned semiconductor fabrication facilities based in China.

Reports further suggest that, shortly before the revocations took effect around December 31, 2025, the U.S. government approved time-limited export licenses permitting continued exports of certain controlled items to the affected facilities. These developments underscore both BIS's continued willingness to tighten end-user controls targeting China's semiconductor sector, and its use of licensing as a mechanism to manage economic and diplomatic consequences. Further, Commerce's framing of the action as closing a "loophole" harkens back to the America First Trade Policy's directive to "eliminate loopholes in existing export controls—especially those that enable the transfer of strategic goods, software, services, and technology" to strategic rivals.

4. Bargaining Chips

Unlike the first Trump administration and the Biden administration, which generally viewed export controls, especially those targeting semiconductors, as specialized national security tools, the second Trump administration has increasingly deployed export controls to gain leverage in broader trade negotiations. In May 2025, BIS reportedly sent letters to three major software companies imposing new license requirements for the export of chip design software to China. These requirements were later removed in July 2025 as part of a negotiated trade deal with Beijing, which Commerce Secretary Lutnick publicly linked to China's agreement to loosen restrictions on exports of rare earth materials.

Export controls were also used as leverage in the White House's negotiations with U.S.-headquartered chip manufacturers, which reportedly made economic concessions to the U.S. government to secure the ability to re-establish sales of certain chip lines to China. As detailed in our recent client alert, BIS issued limited relief for these products in January 2026.

Even with the partial resumption of sales of certain U.S.-made advanced chips to China, BIS enforcement actions in 2025 serve as a reminder that controlling access to AI-capable computing power remains a strategic priority for the United States. The Trump administration's greenlighting of advanced chip sales to China in late 2025 was reported around the same time the U.S. government brought two significant criminal enforcement actions, targeting the illegal export of advanced U.S.-origin chips to China. In November 2025, DOJ announced the arrest and indictment of four individuals who, from September 2023 through November 2025, allegedly transshipped approximately 800 advanced GPUs to China through Malaysia and Thailand without a required export license. In December 2025, DOJ announced that it had successfully dismantled a separate, sophisticated chip-smuggling network exporting advanced GPUs to China and other restricted destinations.

B. End-User Controls

1. Affiliates Rule Issuance and Suspension

In a year marked by significant policy shifts, one of the most consequential developments out of BIS was its issuance and quick suspension of its so-called "Affiliates Rule." Issued as an interim rule on September 29, 2025 with immediate effect, the Affiliates Rule briefly extended certain export controls to foreign affiliates that are 50 percent or more owned by one or more entities on the Entity List, Military End-User (MEU) List, or subject to SDN end-user controls under section 744.8 of the EAR. By some measures, the Affiliates Rule brought another 20,000 unlisted Chinese companies onto restricted lists. On November 12, 2025, however, BIS published a final rule suspending the Affiliates Rule for one year, effective through November 9, 2026.

The promulgation and subsequent suspension of the Affiliates Rule is yet another example of the Trump administration's evolving stance toward China, and its willingness to allow export controls to be included as potential bargaining chips in broader trade negotiations. The Affiliates Rule was intended to address BIS's longstanding "whack-a-mole" problem, under which listed entities often establish "legally distinct" affiliates to evade U.S. export controls. Unlike OFAC's restricted party lists, which have long been interpreted to include affiliates under OFAC's 50 Percent Rule,

prior to the BIS Affiliates Rule's issuance, Commerce's restricted party lists generally applied only to specifically enumerated entities and not to their subsidiaries or affiliates. Given the concentration of China-based entities on BIS's restricted party lists, the Affiliates Rule contributed to heightened U.S.–China trade tensions. The rule's one-year suspension occurred against the backdrop of broader U.S.–China trade negotiations, concluded during the Asia-Pacific Economic Cooperation (APEC) Summit in South Korea.

The Affiliates Rule represents one of the most far-reaching changes to BIS regulations in years. As detailed in our prior alert, the rule:

- **Extends licensing requirements, exceptions, and review policies** to any foreign affiliate owned 50 percent or more by one or more listed entities, whether directly or indirectly, individually or in the aggregate. Conceptually similar to OFAC's 50 Percent Rule, this approach departs from BIS's traditional list-based framework;
- **Imposes the most restrictive license requirements**, license exception eligibility, and license review policy applicable to any of the affiliate's listed owners under the EAR;
- **Imposes heightened due diligence obligations** for exporters, reexporters, and transferors who have "knowledge," including "reason to know," that a foreign counterparty is directly or indirectly owned by a listed entity; and
- **Expands end user-based foreign direct product rules** to restrict transactions with newly "constructively listed" affiliates.

Importantly, the Affiliates Rule has not been repealed. Absent further regulatory action or broader policy changes, the rule will automatically come back into effect on November 10, 2026. The current suspension should therefore be viewed as temporary relief rather than a permanent resolution; affected industries should use this window to prepare for its reinstatement. Many exporters subject to the EAR had already made significant investments to comply with the rule prior to its suspension and have continued to maintain those compliance measures to avoid being unprepared in the event of a snapback.

2. Notable Entity List Designations

BIS continued to prioritize China-related Entity List designations in 2025, adding approximately one hundred entities over the course of the year. Although the overall number of China-related designations was lower than in 2024, the 2025 actions appear to have been more targeted, potentially reflecting BIS's ability to more finely calibrate Entity List additions in light of the far-reaching implications of the Affiliates Rule. Targeted industries and activities included:

- **Advanced chips, quantum, and AI:** BIS designated multiple China-based firms for supporting the development of China's quantum technology sector, warning that such technologies could significantly enhance Chinese military capabilities. In addition, 19 China-based entities, two Singapore-based entities and one Taiwan-based entity were listed for activities related to AI, supercomputing, and high-performance chip development closely tied to Chinese military end users. BIS also designated several Chinese academic and research institutions for their roles in developing large AI models,

quantum technologies, and advanced computing chips contributing to China's military and surveillance capabilities.

- **Hypersonic technology:** BIS designated 34 Chinese entities for acquiring, or attempting to acquire, U.S.-origin items in support of China's development of hypersonic weapons and flight technologies.
- **Russian diversion:** BIS designated at least one Chinese entity for supplying otherwise-prohibited technology to Russian military end users.

BIS also targeted supply chains supporting Iran's UAV programs. In March and October, BIS added 17 China-based entities to the Entity List for providing U.S.-origin components to Iran's defense sector, particularly for use in UAV programs operated by Iranian proxies such as the Houthis and Hamas. In addition, BIS designated three PRC addresses associated with a Chinese individual previously designated by OFAC for supporting a sanctioned supplier of the Iranian military.

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

BIS also appears to be continuing its internal review of proposed military end-user rules issued in 2024 (the Proposed MEU Rules). If adopted, the Proposed MEU Rules would significantly expand the scope of existing military end-user and end-use restrictions to cover *all items* subject to the EAR, including lesser-controlled EAR99 items, and to apply to all countries specified in Country Group D:5 (which includes countries subject to U.S. arms embargoes) as well as Macau.

The Proposed MEU Rules would also prohibit U.S. persons from providing "support" to military end users, intelligence end users, and foreign-security end users as defined or redefined in the proposed rules. If implemented, these provisions would materially alter the treatment of services under the EAR. In particular, cloud-based services—such as IaaS, platform as a service (PaaS), and software as a service (SaaS)—which have traditionally fallen outside the scope of the EAR, could become subject to licensing requirements when provided to covered end users.

C. ITAR Updates

Notable developments in U.S. export controls were not limited to the Commerce Department. Whereas BIS is responsible for overseeing and administering the EAR, controls over the movement of defense articles remain within the purview of the U.S. Department of State, which has responsibility for the International Traffic in Arms Regulations. Through updates to the ITAR, in 2025 the State Department office that administers the regulations, the Directorate of Defense Trade Controls (DDTC), adjusted the items subject to its jurisdiction, implemented U.S. foreign policy goals through both the easing and tightening of license requirements, and took procedural steps to streamline the export licensing process across the U.S. government.

1. ITAR and USML Revisions

DDTC continued to expand coverage of emerging and automated warfare technologies under the United States Munitions List (USML) in 2025, while further offloading civilian munitions and commercially oriented technologies to the EAR. In particular, the State Department issued a final rule, effective September 15, 2025, revising and expanding USML Categories III–V, VII–XIV, XVIII, and XIX–XXI.

This rule represents one of the more significant expansions of the USML in recent years. Among other changes, it added the F-47 (a planned sixth-generation fighter jet) and several other aircraft platforms, certain chemical agents and precursors, uncrewed and untethered vessels, and a broad range of related components and parts to the USML. At the same time, DDTC sought to preserve licensing flexibility for systems with legitimate scientific or commercial applications. For example, the rule excluded from ITAR jurisdiction or provided license availability for certain Global Navigation Satellite System anti-jamming and anti-spoofing systems and Airborne Collision Avoidance Systems antennas. DDTC also introduced a license exemption for qualifying Unmanned Underwater Vehicles designed for commercial uses, such as seabed exploration and the installation and maintenance of undersea infrastructure.

Separately, the State Department updated the licensing policy in ITAR Section 126.1—country-based restrictions that stem from United Nations actions, terrorism-related designations, and arms embargoes—to reflect recent UN Security Council resolutions. This rule revised the licensing policy applicable to the Democratic Republic of Congo, Haiti, Libya, Somalia, the Central African Republic, Sudan, and South Sudan—tightening restrictions in certain cases while easing them in others, in response to the latest developments in conflicts throughout these jurisdictions.

2. Continued AUKUS Adjustments

On December 30, 2025, DDTC further amended the ITAR to streamline defense trade and government-to-government cooperation under the Australia–United Kingdom–United States (AUKUS) partnership. The final rule eliminates the requirement to identify Australian or UK governmental authorities as Authorized Users when relying on the AUKUS-specific license exemption under ITAR Section 126.7.

The rule also introduces a new exemption permitting certain reexports, retransfers, and temporary imports among authorized parties in support of Australian, UK, or U.S. armed forces operating outside of those three jurisdictions. These changes are intended to reduce administrative friction and facilitate closer operational and industrial collaboration among AUKUS partners.

3. Suspended and Lifted Arms Embargoes: Cyprus & Cambodia

In 2025, the United States continued to use the suspension and revocation of arms embargoes as foreign policy tools. On November 7, 2025, DDTC permanently and unconditionally lifted the arms embargo on Cambodia. The embargo had been imposed in 2021 amid concerns regarding rising Chinese influence within the Cambodian military, and its removal marked a notable shift in U.S. policy toward Phnom Penh.

This development contrasts with the more cautious approach taken with respect to Cyprus. In recognition of Cyprus's continued efforts to combat money laundering and restrict Russian naval access to its ports, DDTC suspended the arms embargo on Cyprus for the fourth consecutive year, rather than lifting it outright.

4. Introducing USXPORTS.gov

In November 2025, the Department of State launched USXPORTS.gov, a unified portal for navigating export license applications submitted to both BIS and DDTC. The platform was developed pursuant to Executive Order 14268, which directs those two agencies to reform foreign defense sales to improve speed and accountability.

USXPORTS.gov replaces the two former tracking systems used for DDTC and BIS license applications and provides centralized tracking and visibility across the defense export licensing lifecycle. The portal represents a step toward greater transparency and coordination between the Commerce and State Departments in administering U.S. export control regimes.

D. Licensing Trends

In contrast to efforts to facilitate licensing for foreign military sales, at the outset of his term, President Trump directed BIS to undertake a comprehensive review of the U.S. export control system and imposed a regulatory freeze on a range of Biden-era rules. As part of this review, BIS suspended certain license requirements applicable to advanced computing chips and temporarily paused the acceptance or processing of new license applications, resulting in a significant licensing backlog.

This review process led to several notable adjustments to prior licensing practices. Most prominently, BIS rescinded the AI Diffusion Rule (as discussed above) and revoked a firearms-related licensing rule issued during the Biden administration. The review also coincided with the August 2025 enactment of the Maintaining American Superiority by Improving Export Control Transparency Act, which requires Commerce to submit annual reports to Congress detailing license applications that involve certain restricted end users located in certain jurisdictions (including China, Russia, and other arms-embargoed countries).

Although these developments signal a reassessment of the scope and administration of U.S. export controls, it remains unclear how this sweeping review will ultimately affect BIS's licensing policies and practices. Notably, these changes are occurring against the backdrop of broader agency turnover and loss of institutional memory, driving 2025 processing times for BIS license applications to their highest level in more than 30 years. In particular, questions remain

regarding whether licensing timelines, review standards, and approval rates will stabilize or continue to fluctuate as BIS balances national security objectives, economic competitiveness concerns, and foreign policy considerations. As we discussed recently, although these changes have created uncertainty and presented exporters with day-to-day challenges, this inflection point at BIS also brings potential opportunities for industry to advocate for new approaches.

E. Enforcement Trends

Despite personnel changes and a shifting regulatory environment, BIS maintained a robust export enforcement posture in 2025, as the agency entered into eight settlement agreements with businesses and affiliated individuals, resulting in civil penalties totaling approximately $104 million. Enforcement actions spanned a range of industries, including freight forwarding, aviation, and semiconductor technology, and continued to focus heavily on exports involving China and Russia.

BIS also brought multiple enforcement actions involving unauthorized exports of low-sensitivity EAR99 items, underscoring that export control compliance risks are not limited to highly controlled technologies. These cases reflect BIS's continued emphasis on strict adherence to the EAR's end-use, end-user, and destination-based restrictions, regardless of an item's classification. In addition to civil enforcement actions, BIS continued to deny export privileges to individuals and entities found to have violated U.S. export control laws, or where such denials were deemed necessary to prevent imminent violations.

BIS's $95 million settlement with California-based ***Cadence Design Systems*** (Cadence) was the largest penalty of 2025. Acting through its Chinese subsidiary, Cadence sent EAR-controlled Electronic Design Automation technology for semiconductors to an Entity-Listed Chinese university, without the requisite BIS authorization. The BIS settlement was significantly larger than normal and may represent a warning shot for other companies in the semiconductor industry. Additionally, the penalty amount likely reflects BIS's findings that employees had reason to know the recipient of the controlled technology was a listed entity and that prohibited sales spanned over five years and totaled over $45 million.

The BIS settlement was announced alongside a coordinated resolution with DOJ, as Cadence also became the first company to agree to a corporate guilty plea for a national security offense during the second Trump administration. The more than $140 million in combined criminal and administrative penalties are among the highest ever in an export enforcement case. The multi-agency resolution reflects continued close interagency cooperation in enforcing export controls. Even as other areas of corporate enforcement may see deprioritization, national security-related enforcement, particularly involving sensitive technologies and exports to China and other countries of concern, continues to accelerate.

The Cadence matter stands in contrast to two other DOJ resolutions this year, which emphasize the potential benefits of voluntary self-disclosure, cooperation, and remediation under the National Security Division's (NSD) enforcement policies:

- In April 2025, pursuant to its Enforcement Policy for Business Organizations, NSD declined to prosecute ***Universities Space Research Association***, a nonprofit research organization and NASA contractor, after the company promptly disclosed misconduct by a former employee who had willfully provided EAR99 flight control software to an Entity List party in China. NSD cited the organization's timely and voluntary disclosure, exceptional cooperation, and meaningful remediation as key factors supporting the declination.
- A second declination, announced in June 2025, involved ***White Deer Management's*** (White Deer) acquisition of ***Unicat Catalyst Technologies*** (Unicat). Following the acquisition, White Deer discovered chemical catalyst sales by Unicat to customers in Iran, Syria, Venezuela, and Cuba in violation of U.S. export control and sanctions laws. NSD declined to prosecute White Deer under its Voluntary Self-Disclosures in Connection with Acquisitions Policy (its first-ever declination under this policy), citing White Deer's prompt disclosure, proactive cooperation, and remediation within a year of discovering the misconduct. Notably, NSD reached this outcome despite aggravating factors at Unicat, including senior management involvement. Unicat itself entered into a non-prosecution agreement with DOJ, receiving credit for White Deer's actions, while Unicat's former CEO pleaded guilty.

Looking ahead to 2026, BIS is expected to continue expanding enforcement efforts to advance U.S. national security objectives, with a particular focus on exports to U.S. adversaries—especially China—and on sensitive technologies such as AI, quantum computing, hypersonics, and semiconductors. Signaling its concerns regarding these risks, Congress has increased BIS's budget by 23 percent, or approximately $44 million, in 2026, with the majority of that funding earmarked to support additional enforcement personnel. DOJ is similarly expected to continue prioritizing the criminal enforcement of export control and other national security-related offenses, with U.S. Attorney's Offices and DOJ's Criminal Division supplementing NSD's efforts.

F. Other BIS Regulatory Regimes

Separate from U.S. export controls administration, other offices within BIS sought to innovate in their enforcement of long-standing prohibitions, and to address emerging threats through the implementation of new regimes.

1. Antiboycott Compliance

BIS's Office of Antiboycott Compliance (OAC) continued to publish updates to its Boycott Requester List in 2025. First announced in March 2024 to facilitate compliance with U.S. antiboycott requirements, the Boycott Requester List serves as a public repository of entities that have made reportable boycott-related requests—including requests to comply with the Arab League boycott of Israel—that have been submitted to BIS. The list is intended to provide U.S. persons, as well as foreign persons subject to the reporting requirements of Part 760 of the EAR, with notice that identified counterparties may present an elevated risk of making reportable boycott-related requests.

Importantly, inclusion on the Boycott Requester List does *not* prohibit U.S. persons from engaging in transactions with listed entities. Rather, the list functions as a compliance aid, highlighting the need for heightened vigilance and internal controls when dealing with identified parties. Entities may be removed from the list by submitting an attestation to OAC confirming that they have eliminated boycott-related language from purchase orders, contracts, letters of credit, and other commercial communications with U.S. persons and their foreign subsidiaries.

OAC has indicated that the Boycott Requester List is updated quarterly. BIS's press release in April 2025 followed the practice of the Biden administration, identifying the number of additions to and removals from the list during the prior quarter. BIS stated that, since the introduction of the list, more than 65 entities have agreed to discontinue the inclusion of boycott-related terms in their transactions with U.S. persons, underscoring the list's role as both a compliance tool and an enforcement-adjacent mechanism incentivizing voluntary remediation. Although the current version of the Boycott Requester List—which includes 181 parties as of this writing—indicates that OAC made further additions across 2025, BIS appears to have ceased its public releases regarding the quarterly updates.

BIS brought one antiboycott enforcement action in 2025, assessing a $44,750 civil penalty against a Florida-based defense contractor. The company voluntarily disclosed and agreed to settle charges relating to three alleged violations arising from a 2019 transaction, including furnishing information about business relationships with a blacklisted party, and failing to report receipt of two boycott-related requests as part of the same transaction (specifically, a certification stating that "no labor, capital, parts, or raw materials of Israeli origin have been used" in connection with the goods, and stating that certain parties were not included "on the Israeli Boycott Blacklist").

As in other corners of BIS, OAC experienced significant leadership changes in 2025, with the departure of longstanding office leader Cathleen Ryan. Given the small size of BIS's antiboycott team and the high level of engagement Director Ryan had in its activities, this change may have a significant impact on how the agency reviews boycott reports, approaches disclosures and enforcement, and on its willingness to provide industry guidance via its hotline, which was often staffed directly by Director Ryan.

2. ICTS Regulations

BIS's Office of Information and Communications Technology and Services (OICTS) continued its efforts to address national security concerns in ICTS supply chains. Most notably, in 2025, OICTS issued a final rule prohibiting certain transactions involving "connected vehicles" and related components with a sufficient nexus to China or Russia (the Connected Vehicles Regulations). With some of these prohibitions impacting Model Year 2027 vehicles, 2026 will be a critical year for importers and manufacturers involved in the connected vehicles supply chain to review and potentially enhance their policies and procedures to ensure ongoing compliance.

OICTS also issued an advance notice of proposed rulemaking (ANPRM) soliciting comments on efforts to restrict the use of Chinese- and Russian-origin unmanned aerial systems and related components, though additional regulatory action by OICTS has not yet occurred. Any future efforts will likely complement the U.S. Federal Communications Commission's (FCC) December

2025 addition of most foreign-made uncrewed aircraft systems and related critical components to the FCC's Covered List—which prohibits such items from receiving FCC equipment authorization and thus effectively restricts their entry into, or sale or marketing within, the United States. In the coming year, we expect OICTS to continue its rulemaking efforts in the drone space and potentially in other sectors, including IaaS transactions. However, recent leadership flux, including the January 2026 departure of inaugural OICTS Director Elizabeth Cannon, may result in new regulatory priorities.

a) Connected Vehicles Regulations

As discussed in detail in our previous client alert, the Connected Vehicles Regulations prohibit the import and sale in the United States of certain "connected vehicles" and key components, including Vehicle Connectivity Systems (VCS) and Automated Driving Systems (ADS) linked to Chinese-affiliated or Russian-affiliated companies. Broad prohibitions on the sale of "connected vehicles" by manufacturers with a sufficient nexus to China or Russia, even if manufactured in the United States, apply to Model Year 2027 vehicles. Although these regulations currently only apply to passenger vehicles under 10,001 pounds, a similar rule for commercial vehicles is expected. Additional software-related prohibitions will also take effect for Model Year 2027 vehicles, and hardware-related prohibitions will take effect for Model Year 2030 vehicles, or on January 1, 2029 for units without a model year.

Importantly, the Connected Vehicles Regulations require VCS hardware importers and connected vehicle manufacturers to submit declarations of conformity to BIS at least 60 days prior to the first import or sale of items associated with a particular vehicle model or calendar year beginning with Model Year 2027 vehicles. These declarations require detailed descriptions of supply chains, country of origin, associated foreign interests—including non-Chinese and non-Russian foreign interests—and due diligence steps relating to the covered items. These declarations can be submitted through BIS's Compliance Application and Reporting System (CARS) webpage. In the coming years, affected companies will similarly need to submit declarations of conformity at least annually, conduct supply chain due diligence to ensure compliance with the Connected Vehicles Regulations, and keep records of relevant transactions for up to 10 years.

BIS is empowered to issue general and specific authorizations to allow transactions otherwise prohibited by the Connected Vehicle Regulations, and parties may also request guidance as to whether a prospective transaction is prohibited through an advisory opinion process. Additional information can be found on BIS's dedicated Connected Vehicles webpage.

Despite the staggered implementation dates, 2026 will be a watershed year for connected vehicle manufacturers and associated companies, which will have to review (and possibly modify) their software and hardware in order to ensure their vehicles and ADS and VCS systems, parts, and components remain in compliance for import into the United States.

b) Other Possible OICTS Rulemaking Efforts

As noted above, OICTS also issued a separate ANPRM involving unmanned aerial systems and related components in 2025. Unlike a notice of proposed rulemaking (NPRM), ANPRMs

generally do not propose specific regulatory solutions, but instead solicit comments on the scope of an issue and how to address it. This ANPRM solicited public comments on how to address national security risks related to drone systems, including which forms of Russian- and Chinese-origin ICTS pose the greatest vulnerabilities and which ICTS functionalities are most integral to the functionality of these systems. The ANPRM generated substantial interest from a wide range of stakeholders, including over 600 public comments. Given recent and ongoing efforts by BIS and the FCC to regulate drone system technology linked to China, we expect OICTS to continue its focus on this area and potentially engage in further rulemaking activities. Such efforts could have potentially wide-ranging impact on drone users—ranging from photographers to farmers to local government and emergency response agencies—and stakeholders should continue to monitor this space carefully for possible further action in 2026.

The regulation of IaaS and training of large AI models is yet another area of potential OICTS rulemaking activity in the coming year. In 2024, OICTS issued a notice of proposed rulemaking aimed at the activities of U.S. IaaS providers, including the training of large AI models. As discussed in our client alert, if unchanged, the rule would require U.S. IaaS providers (1) to report certain transactions involving foreign persons and large AI models and (2) to implement extensive compliance measures, including establishing customer identification programs to collect, verify, and maintain information about their foreign customers, among other compliance steps. Over 500 public comments were submitted in response to this NPRM, though no further rulemaking activity has occurred to date. The regulation of AI and IaaS were previously identified as key priorities for OICTS, and further actions in this space are possible this year, though the organizational priorities of the new OICTS leadership remain to be seen.

III. U.S. FOREIGN INVESTMENT RESTRICTIONS

Review of foreign direct investment in the United States and stricter controls on U.S. capital outflows to certain destinations remained key priorities throughout 2025. As an early signal of the second Trump administration's investment policy objectives, in February 2025, the White House issued a National Security Presidential Memorandum, the "America First Investment Policy," proposing changes to the regulations for the Committee on Foreign Investment in the United States (CFIUS or the Committee) and the nascent Outbound Investment Security Program (OISP). Drawing a connection between economic security and national security, the America First Investment Policy envisions a "strong, open investment environment," which is backed by an unprecedented CFIUS "fast track" to facilitate greater investment from allies and partners, while simultaneously heightening protections against national security threats posed by "foreign adversaries"—most notably, China. The Assistant Secretary of the Treasury for Investment Security's recent confirmation hearing indicates that CFIUS and OISP enforcement will continue to remain key priorities for the second Trump administration.

A. Inbound Investment

1. Release of CFIUS Annual Report for 2024

CFIUS—the interagency panel tasked with reviewing the national security risks associated with foreign investment in U.S. companies—celebrated its 50th anniversary in 2025. Before turning to the year just ended, we note a few key trends from CFIUS's 2024 annual report (the CFIUS

Annual Report), which was released in August 2025 and outlines the Committee's activity during the final year of the Biden administration:

- **There was a slight decline in CFIUS's overall caseload, paired with a small increase in the use of short-form declarations**: The Committee reviewed or assessed a total of 325 "covered transactions"—CFIUS's jurisdiction extends to transactions that result in a foreign person obtaining "control" of a U.S. business, as well as certain non-controlling but non-passive covered investments in a "TID U.S. business" that performs certain activities involving critical technologies, critical infrastructure, or sensitive personal data. 2024 marked the second consecutive decline in overall filings, as the global mergers and acquisitions (M&A) market only slowly began to recover from the lows of 2023. The 116 declarations (i.e., a short-form CFIUS filing that is intended to ease the administrative burden on transaction parties, as compared to the long-form CFIUS filings known as notices) represent a modest increase from the 109 declarations submitted to the Committee in 2023. The declarations included six real estate filings and 36 mandatory filings, with 17 declarations ultimately resulting in a request for a notice. Looking ahead, the Trump administration's stated emphasis on streamlining CFIUS review, as reflected in the America First Investment Policy, is likely to reinforce the continued use of declarations for lower-risk transactions, particularly those involving investors from allied countries and routine filers.

- **CFIUS's enforcement activity took center stage (but perhaps not for long):** The Committee assessed a record five monetary penalties in 2024, as reported in the CFIUS Annual Report, including the largest penalty issued to date: $60 million for breach of a mitigation agreement (i.e., deal-specific restrictive covenants to mitigate national security risk upon which CFIUS often conditions its approval of transactions). These enforcement efforts coincided with the Treasury Department's November 2024 final rule that expanded CFIUS's penalty and subpoena authorities and formalized strict timelines for parties to negotiate mitigation agreements. However, despite a blockbuster enforcement year in 2024, 2025 saw no public announcements from the Committee regarding new penalties in connection with enforcement actions—though the recently-confirmed Assistant Secretary of the Treasury for Investment Security stated in his confirmation hearing that reviews of non-notified transactions will remain a priority for the Trump administration.

- **New mitigation agreements are in decline:** As of the end of 2024, CFIUS was monitoring 242 ongoing mitigation agreements and conditions. Throughout 2024, however, CFIUS required mitigation in 16 transactions, a significant decline from the 35 transactions in 2023. This downward trend may continue considering the America First Investment Policy, which notes that the Trump administration will "cease the use of overly bureaucratic, complex, and open-ended 'mitigation' agreements for United States investments from foreign adversary countries," in order to "reduce uncertainty for investors, reduce administrative burden, and increase Government efficiency."

- **Non-notified reviews remain a central focus and growing risk:** CFIUS's investigative engine remained active and well-resourced in identifying "non-notified transactions" (i.e., transactions that are potentially within CFIUS jurisdiction for which the parties did not file a notice or declaration). In 2024, CFIUS conducted preliminary review of thousands of transactions, investigated 98 non-notified transactions, and ultimately opened 76 formal inquiries—an increase from 60 such inquiries in 2023. From these inquiries, CFIUS requested filings in 12 cases, and in five additional instances parties received non-notified outreach from CFIUS and voluntarily filed a declaration or notice before receiving a formal request. The May 2024 presidential order prohibiting and ordering the unwinding of the ***MineOne Partners*** real estate transaction, which originated through the

non-notified review process, provides a stark example of the risks of forgoing even voluntary CFIUS filings when transactions raise U.S. national security concerns.

- **France, Japan, and the United Arab Emirates were frequent filers:** When measured by individual, distinct transactions, the top notice filers in 2024 were France, Japan, and the United Arab Emirates. Although Chinese investments were the subject of 26 notices, China does not rank among the top notice filers once the data is adjusted to account for double counting (i.e., counting each transaction only once where a transaction was initially submitted as a declaration and later re-filed as a notice, or where a notice was re-filed one or more times). As CFIUS continues to subject Chinese investments to heightened scrutiny, the result appears to be relatively few approvals and a decreasing appetite by parties to submit Chinese-investor transactions for Committee review.

2. Fast-Track Pilot Program

Among the most notable procedural changes to CFIUS by the Trump administration in 2025, the America First Investment Policy previewed a new "fast-track" program to expedite the CFIUS review process for certain filers, through the use of a "Known Investor" portal (KIP). A KIP pilot program, announced in May 2025, is currently collecting pre-filing information from certain foreign investors to establish baseline relationships between parties who make filings frequently with the Committee. The KIP and its eligibility criteria are still being developed, but, as noted in the Treasury Department's Frequently Asked Questions (FAQs), CFIUS anticipates that eligibility will depend on the foreign investor's filing frequency and "certain questions related to its business and activities." As noted in our prior client alert, we anticipate the KIP program could be particularly valuable for European and Middle Eastern investors, particularly for transactions with minimal national security risks.

3. Lessons Learned from Nippon Steel and HieFo

After an eighteen-month-long legal battle, President Trump approved Japan-based ***Nippon Steel's*** acquisition of ***U.S. Steel***. The $15 billion deal was first signed over two years ago and faced scrutiny from the United Steelworkers and bipartisan opposition, as both President Trump and President Biden made clear their intent to block the acquisition, in a potentially paradigm-shifting politicization of the CFIUS process. In January 2025, during his final few weeks in office, former President Biden prohibited the deal. Then, in April 2025, President Trump publicly directed the Committee to conduct a first-ever *de novo* review of the transaction.

In June 2025, President Trump ultimately approved the acquisition, subject to a mitigation agreement. The most noteworthy detail from the mitigation agreement that has emerged is a so-called "golden share" to be held by the U.S. government. Golden shares, which provide governments with (typically non-economic) stakeholder rights in companies, have previously been used outside of the United States, particularly in the defense industry and with respect to the privatization of "national champions." To our knowledge, this is the first time that CFIUS has included a golden share in a mitigation agreement, but the requirement is in accord with the Trump administration's more forward-leaning approach with respect to taking stakes in private enterprises. Considering the new guidelines for mitigation agreements announced in the America First Investment Policy, the Nippon Steel–U.S. Steel agreement could foreshadow what other new mitigation agreements might look like under the second Trump administration.

Despite the novel approach to Nippon Steel, the Trump administration continues to heavily scrutinize transactions that it determines may pose significant national security risks, including ordering ***HieFo Corporation***, a Delaware-incorporated entity controlled by Chinese investors, to completely divest its acquisition of the digital chips and related wafer design, fabrication, and processing businesses of ***EMCORE Corporation***, a transaction that closed in April 2024. Only nine such divestiture orders have occurred in the past decade, three of which have occurred in the past two years alone.

4. Lingering Impact of the U.S. Government Shutdown

The longest government shutdown in U.S. history, lasting a total of 43 days in late 2025, had widespread impacts across the operations of the U.S. government, and the Treasury Department was no exception. The acceptance and adjudication of CFIUS filings in 2025 was formally stalled during the shutdown, resulting in delays in CFIUS reviews and clearances. Most external-facing CFIUS deadlines are tolled during a shutdown, leaving transaction parties with extended deal timelines and sometimes the need to close over required approvals.

B. Outbound Investment

2025 marked the inaugural year of the Outbound Investment Security Program, a set of regulations issued by the U.S. Department of the Treasury under the Biden administration, which restricts certain U.S. investments in critical technology sectors in China. As 2025 came to a close and President Trump signed into law the National Defense Authorization Act (NDAA) for Fiscal Year 2026, the OISP is now codified and statutory changes to the scope of the restrictions are set to be implemented by March 2027. Over the next year, U.S. investors will continue to seek clarity on the coverage of the current regime, while preparing for future changes to take effect.

1. Initial Implementation and Compliance Standards

Effective January 2, 2025, the OISP restricts outbound investments (covered transactions) by U.S. persons into certain companies in or with operations in China (including Hong Kong and Macau), or owned by or affiliated with, Chinese persons (such companies, covered foreign persons), in the semiconductors and microelectronics, quantum information technology, and AI sectors. As described in prior client alerts, certain covered transactions are outright prohibited, while others merely require a notification to the Treasury Department providing details of the investment. The OISP does not review and then approve or deny transactions, as in the CFIUS context. Rather, the obligation is on U.S. persons to avoid engaging in prohibited transactions or file notifications with Treasury where required, and to discern the difference. The OISP is administered by a newly established Office of Global Transactions within Treasury (and sits within the same Office of Investment Security that houses CFIUS). The Office has released several rounds of FAQs regarding the OISP over the past year as industry has sought greater clarity on the new regime.

The top-line impact of the OISP is that U.S. persons must now contend with new compliance challenges in considering investments involving some of the highest-growth sectors of China's economy. For example, covered activity includes the development of AI systems intended to control robotic systems. Given the ubiquity of automation across Chinese industry and the increasing use of AI to guide such systems, potential investments in sectors once considered outside of the OISP's scope (e.g., autonomous vehicles or manufacturing) may now, or could soon, constitute covered investments.

We observed a trend towards overcompliance in the first half of 2025, as industry wrestled with the scope and impact of the OISP regulations. This included a general reluctance to engage in investments in the covered sectors, whether or not the transaction would be notifiable or prohibited, as well as the inclusion of OISP-related representations and warranties in investment structures seemingly far removed from OISP jurisdiction. Over the course of the year, however, these growing pains appeared to ease.

Commercial opportunities, at least in the initial public offering (IPO) space, appear to be a major driving force in U.S. persons testing the waters with notifiable or exempted transactions. The IPO market in Hong Kong, a preferred destination for Chinese companies seeking international investors, experienced a significant rebound this past year. 2026 appears poised to be another blockbuster year, with over 300 IPO applications currently in the pipeline to be listed on the Hong Kong exchange. Given the potential for investment returns and fees in connection with such listings, U.S. persons are increasingly either filing notifications or getting more comfortable relying on the "publicly traded securities" exception, which generally excepts transactions from the OISP regulations where the U.S. person is acquiring publicly traded securities. FAQs published by the Treasury Department in December 2025 indicate that the Treasury Department is interpreting the availability of the publicly traded securities exception more favorably.

Yet, with a lack of public enforcement actions or major trade association guidance to serve as a benchmark for due diligence expectations, many questions remain. As more notifications are filed and more U.S. investors engage with the Treasury Department on the contours of the rules, we could expect additional OISP-related FAQs and guidance in 2026, perhaps in conjunction with promulgation of the regulatory amendments called for under the NDAA.

2. Codification and Future Expansion

President Trump's America First Investment Policy foreshadowed a potential expansion of the OISP, directing that covered sectors be "reviewed and updated regularly" and indicating that certain exceptions may be narrowed. The U.S. Congress, which has been trying to pass more restrictive outbound requirements for several years, finally got across the finish line with the inclusion of the Comprehensive Outbound Investment National Security Act of 2025 (the COINS Act) as part of the NDAA for Fiscal Year 2026. The COINS Act codifies essential elements of the current OISP, but empowers, and, in some cases requires, the Treasury Department to expand the OISP's scope.

These changes in the COINS Act are not self-executing—rather, the Secretary of the Treasury is directed to issue implementing regulations within 450 days (i.e., by March 2027), though such regulations could be issued sooner and possibly as a final rule with immediate effect. Among the COINS Act's notable changes to the current OISP regime are:

- **Expanded geographic and technological scope**: The COINS Act looks beyond the PRC (including Hong Kong and Macau), adding Russia, Iran, North Korea, Cuba, and Venezuela "under the regime of" Nicolás Maduro to the list of "countries of concern" within the scope of the regulations. This expanded list is consistent with the approach taken in other recent regulations, notably the DOJ's Data Security Program that came into effect in April 2025. The list of covered technologies is also broadened to add high-performance computing/supercomputing and hypersonic systems, and the act grants the Secretary of the Treasury authority to identify additional types of prohibited or notifiable technologies going forward.

- **Changes to covered foreign persons definition:** The COINS Act amends the definition of covered foreign persons to include a person "subject to the direction and control" of: foreign persons incorporated in, with a principal place of business in, or organized under the laws of a country of concern, or the governments or political leadership of countries of concern (including members of the Central Committee of the Chinese Communist Party with respect to China). This definitional change could ultimately expand the scope of entities to which the OISP applies, but the impact will likely hinge on Treasury's interpretation of "direction" and "control." In this case, the Office of Global Transactions could turn to its Treasury sister agency—OFAC—and that agency's experience in assessing similar terms in the sanctions context.

- **Additional exemptions from OISP jurisdiction, including allowing full underwriting services to covered foreign persons:** The current regulations prohibit U.S. persons from providing underwriting services for IPOs if the U.S. person also acquires equity as part of the process. This is in part because Treasury would consider such services to provide the covered foreign person with market making benefits, or what the Treasury Department describes as "intangible benefits," such as "enhanced standing and prominence, managerial assistance, access to investment and talent networks, market access, and enhanced access to additional financing." The COINS Act will explicitly exempt such underwriting services even with the temporary acquisition of equity. If implemented without amendment or other qualification, this underwriting exemption would provide an even more expansive exemption for U.S. persons to participate in covered foreign person IPOs and would call into question the continuing viability of the "intangible benefits" concept as a restrictive element.

- **New channels of communication with Treasury:** The COINS Act directs Treasury to create a framework for OISP voluntary self-disclosures, similar to other U.S. regulatory regimes, and authorizes Treasury to institute a system to provide non-binding feedback to requesting parties as to whether a potential transaction would constitute a covered transaction.

With the recent confirmation of the Assistant Secretary of the Treasury for Investment Security, we expect the Treasury Department to move swiftly to implement the COINS Act and potentially increase its monitoring and enforcement of the OISP.

IV. U.S. IMPORT RESTRICTIONS

A. Tariffs

In 2025, the second Trump administration fundamentally reoriented U.S. tariff policy, which had been largely static for decades. The first Trump administration accepted existing, often very low, tariff rates, and even signed the United States–Mexico–Canada Free Trade Agreement (USMCA), providing for duty-free treatment for the majority of trade involving the three countries. Exceptional tariffs were imposed by the administration on top of those low rates through specific, long-standing tariff authorities that provide for increased tariffs when the administration determines that the authority's criteria have been met, after lengthy investigations, notice-and-comment periods, and hearings. In short, although the first Trump administration demonstrated an aggressive trade policy, this policy was based on the use of traditional trade authority that limited executive action.

The second Trump administration took the unprecedented step of invoking the International Emergency Economic Powers Act (IEEPA)—the principal statutory basis for modern U.S. sanctions—to impose tariffs on partners and adversaries alike, without any need for prior notice, investigation, or public comment. In order to trigger IEEPA's authorities, the administration must simply declare a "national emergency" that involves, among other things, an "unusual and extraordinary threat" to the "national security, foreign policy, or economy" of the United States. Once such a national emergency is declared, the President may, among other actions, "regulate . . . importation or exportation of . . . any property in which any foreign country or a national thereof has any interest." IEEPA makes no reference to tariffs or duties and had never previously been deployed as a basis for imposing additional import duties.

What began shortly after President Trump's return to office with "trafficking tariffs" tied to declared fentanyl and border-security national emergencies involving Canada, Mexico, and China, evolved into a flexible, executive-driven tariff toolkit that would eventually be used on virtually the entire world (through the declaration of various national emergencies). Thereafter, the administration used IEEPA to impose, modify, and leverage tariff rates at a speed and scale not seen in modern U.S. trade policy, and with profound consequences for global trade and international relations—triggering numerous legal challenges which, as of this writing, are pending before the U.S. Supreme Court.

1. IEEPA-Based Tariffs and U.S. Supreme Court Challenge

From trafficking tariffs to worldwide reciprocal tariffs. Beginning in early February 2025, the United States imposed IEEPA-based duties on imports from China, Canada, and Mexico—generally 10 to 25 percent at inception, subject to limited exceptions—based on the declaration of national emergencies tied to fentanyl imports and immigration concerns, with multiple rounds of pauses, increases, and other adjustments tied to negotiations (or the lack thereof).

On April 2, 2025—so-called "Liberation Day"—President Trump issued Executive Order 14257, declaring a separate national emergency under IEEPA tied to persistent U.S. goods trade deficits. Pursuant to this emergency, the United States then imposed "reciprocal tariffs" on virtually all U.S. trading partners, even those with which the United States did not maintain a

trade deficit. The reciprocal tariff regime established a 10 percent baseline duty on most imports (stacking on top of the existing tariff rate applicable to any given good, sometimes referred to as the "normal" or "most favored nation" rate) from most countries, with dozens of higher, country-specific rates (ranging from 11 to 50 percent). Although the Trump administration soon suspended the country-specific rates for most jurisdictions (while retaining the 10 percent baseline, and maintaining heightened duties for China) and invited trading partners to seek negotiated relief, the breadth and speed of the initial rollout—and the persistence of the baseline duty—generated significant cost shock and uncertainty. Those effects quickly rippled through pricing, contracting, and supply-chain planning.

Rapid rate changes and deal-making leverage. IEEPA tariff rates remained volatile thrughout 2025, with China providing the clearest illustration. Following "Liberation Day," reciprocal tariffs escalated rapidly amid tit-for-tat retaliation between Washington and Beijing—reaching a peak of 125 percent (with the effective rate for many goods substantially higher)—before a partial reset in May 2025, when a joint statement and related executive actions moved tariffs back toward the "baseline," while leaving separate IEEPA-based trafficking duties in place. A later round of talks in the fall produced additional adjustments, including reductions to fentanyl-related IEEPA duties and further suspension of heightened China-specific reciprocal rates.

At the time of this writing, all imports from China are subject to a 10 percent reciprocal tariff and a 10 percent fentanyl tariff, stacking together for a combined 20 percent tariff rate, which applies on top of the normal tariff rate for merchandise in the U.S. tariff schedule, as well as any item-specific Section 301 or 232 tariffs. Consequently, many items from China are presently subject to an effective U.S. tariff rate of 45 percent or more.

More broadly, the Trump administration has used the President's asserted authority to impose and adjust IEEPA-based tariffs essentially at will, as negotiating leverage with a wide range of trading partners, resulting in trade deals we discuss further below.

The Supreme Court challenge. The Trump administration's unprecedented use of IEEPA to impose the trafficking tariffs and worldwide reciprocal tariffs promptly invited statutory and constitutional challenges in U.S. courts.

Importers and states filed suits in the U.S. Court of International Trade (CIT) and in the U.S. District Court for the District of Columbia (among other venues). In May 2025, both courts found the IEEPA tariffs unlawful, and in August 2025, the U.S. Court of Appeals for the Federal Circuit affirmed the CIT decision in a seven-to-four vote. The U.S. Supreme Court granted expedited review on September 9, 2025, consolidated the cases, and heard oral argument on November 5, 2025.

Petitioners make three principal arguments in support of their claim that the President's authority under IEEPA to "regulate . . . importation" does not authorize the President to impose duties. First, as a matter of statutory construction, the asserted "national emergencies" (particularly decades-long U.S. trade deficits) do not constitute the "unusual and extraordinary threat" that IEEPA requires, and further the authority to "regulate" importation does not encompass the ability to collect duties, as opposed to the non-tariff actions that have historically been taken under IEEPA. Second, as a form of taxation, duties are within the exclusive

constitutional purview of Congress, unless specifically "delegated." And although Congress can and has chosen to delegate some tariffing authority to the Executive, it must do so through more specific and procedurally bounded statutes—as it has historically. Third, under the "major questions doctrine," Petitioners argue that the administration improperly resolved an issue of "vast economic and political significance" without clear, explicit authorization from Congress.

The government's counter-arguments include claims that the authority to regulate importation in declared national emergencies naturally and reasonably encompasses setting tariffs, that earlier courts had confirmed that other laws with the same language as IEEPA authorized Executive-promulgated tariffs in addition to the statutory trade authorization that Congress has granted (discussed further below), and that IEEPA's statutory safeguards are sufficient to address non-delegation concerns.

A decision from the Supreme Court could be issued any time between February 2026 and the end of the Court's term in June 2026. In the event the Supreme Court rules the IEEPA-based tariffs impermissible, importers are expected to seek an estimated $150 billion in tariff refunds (an amount that grows with each passing day), although the process for doing so (if at all) is yet to be determined. As importers seek to address uncertainty regarding how to qualify for a refund, hundreds of CIT cases have already been filed by importers seeking to preserve their rights. A victory for President Trump, on the other hand, has the potential to greatly expand Executive emergency powers.

2. Other Tariff Authorities (Section 232, Section 301, Section 122)

Even if IEEPA-based tariffs are curtailed or struck down, traditional tariff authorities—particularly Section 232 of the Trade Expansion Act of 1962 and Section 301 of the Trade Act of 1974—would remain durable, congressionally delegated, and judicially affirmed tools capable of delivering substantial, targeted tariff outcomes. These authorities have been used to advance focused trade and industrial policy objectives across strategic sectors, and courts have repeatedly upheld their use and the Executive's flexibility to adjust related tariff measures over time. As actions over the last few months underscore, while these tools are narrower than sweeping IEEPA-based duties, they can still yield meaningful leverage over foreign governments and firms. Moreover, as we described in a prior client alert, we assess that if IEEPA tariffs become unavailable, the Trump administration could quickly leverage these other statutory authorities to increase duties on a substantial proportion of U.S. imports, replacing all or a portion of the IEEPA tariffs.

Section 232 of the Trade Expansion Act of 1962 authorizes the U.S. Department of Commerce, on its own initiative or at the President's direction, to investigate whether imports of particular products threaten to impair U.S. national security and to recommend action, including tariffs. The Commerce Department has 270 days to complete its investigation and deliver findings and recommendation for action, following which the President has 90 days to determine the action to be taken, which must then be implemented within 15 days. However, all steps can be completed more quickly than this if the administration desires; there is no statutory delay period.

In 2025, the Trump administration directed Section 232 investigations of, and ultimately imposed sector-specific tariffs on: (1) copper derivatives (50 percent on covered products), (2) softwood lumber and derivative products (10 percent global tariff on softwood lumber, with higher tariffs scheduled on upholstered furniture, kitchen cabinets, and vanities that were later terminated), (3) medium- and heavy-duty vehicles and parts (25 percent, plus 10 percent on buses), and (4) semiconductors (25 percent, unless intended for specific U.S.-based end uses). In addition, the White House threatened—and then walked back—100 percent tariffs on branded, patented pharmaceuticals, after extracting commitments related to U.S. investment, domestic capacity, and pricing from at least nine companies. A broad pipeline of Section 232 investigations remains pending.

Section 301 of the Trade Act of 1974 authorizes the U.S. Trade Representative (USTR) to investigate whether a foreign government's trade practices violate trade agreements with the United States or are unjustifiable, unreasonable, or discriminatory and burden or restrict U.S. commerce—following which the President may impose tariffs or take other action to eliminate the practice.

In 2025, USTR used Section 301 to investigate China's maritime, logistics, and shipbuilding practices. In April 2025, USTR issued affirmative findings and proposed countermeasures, including port-service fees and duties on ship-to-shore cranes. The Trump administration later offered Section 301 relief as part of a broader U.S.–China détente that included Chinese commitments to resume or expand purchases of U.S.-origin goods and approve export license applications for certain critical minerals.

In addition to these measures, **Section 122** of the Trade Act of 1974, while never used to date, would allow the President to impose up to 15 percent additional tariffs on imports from any source for a period of 150 days, extendable by act of Congress. This express authority for tariff increases to deal with "balance of payments deficits," the ostensible aim of the IEEPA reciprocal tariffs, has been among the arguments that IEEPA was not intended to provide such authority.

3. End of the *De Minimis* Rule

The Trump administration's reshaping of the U.S. tariff framework has extended beyond rates to regulatory procedures. Of note, President Trump issued Executive Order 14324 suspending duty-free *de minimis* treatment for low-value imports from all countries as of August 29, 2025. This followed the Trump administration's April 2025 targeted removal of *de minimis* treatment for Chinese-origin goods.

The *de minimis* exemption has roots in the Tariff Act of 1930 and historically was intended to "avoid inconvenience and administrative expenses disproportionate to the amount of revenue the government was collecting on imports." Over time, bipartisan concern about the *de minimis* rule emerged, particularly after the threshold to receive duty-free treatment was increased from $200 to $800 per shipment in 2016, resulting in increasing reliance on the exemption by direct-to-customer e-commerce platforms (including China-based "fast fashion" businesses facing forced labor-related allegations). In September 2024, the Biden administration acknowledged an

"exponential increase" in *de minimis* shipments over the prior decade, from approximately $140 million to more than $1 billion annually.

Since the suspension took effect, U.S. Customs and Border Protection (CBP) has reportedly collected approximately $1 billion in duties across roughly 246 million low-value shipments. Effective July 1, 2027, as required by the "One Big Beautiful Bill," passed by Congress and signed by President Trump in July 2025, the *de minimis* rule will be formally repealed (not merely suspended).

4. Tariff Evasion Enforcement and the Trade Fraud Task Force

The emergence of tariffs as the central tool of the America First Trade Policy has been complemented by DOJ's identification of tariff evasion as one of its top criminal enforcement priorities. As we noted in a webcast and an earlier client alert, DOJ and the U.S. Department of Homeland Security (DHS) jointly launched a Trade Fraud Task Force in August 2025, designed to streamline investigations of customs-related misclassification, undervaluation, and false country-of-origin claims.

To uncover tariff evasion schemes, the government relies heavily on tips from DOJ's Corporate Whistleblower Awards Pilot Program (expanded in May 2025 to include trade, tariff, and customs fraud), CBP's e-Allegations Program, and companies' voluntary self-disclosures and prior disclosures. Moreover, the government may intervene in *qui tam* lawsuits filed by private citizens (relators) under the False Claims Act, which provides for treble damages and financial awards to relators. For example, in December 2025, DOJ resolved a case under that statute for $54.4 million, after joining a *qui tam* lawsuit in which a relator alleged the company misclassified Chinese products as originating from Taiwan.

5. Notable Trade Deals

Since "Liberation Day" in April 2025, the Trump administration has announced a series of trade deals with multiple countries. In a departure from traditional trade negotiations, none of these deals were pre-authorized or formally ratified by the U.S. Congress, nor does Congress appear to have played a meaningful role in their negotiation.

As of December 2025, the Trump administration had reportedly concluded or is in the process of reaching trade deals (often styled as a Framework for an Agreement) with Argentina, Ecuador, El Salvador, Guatemala, Cambodia, the EU, Indonesia, Japan, Malaysia, South Korea, Thailand, Switzerland and Liechtenstein, the United Kingdom, and Vietnam. While specific terms vary, these deals generally involve commitments by the foreign counterparty to (1) invest in the U.S. economy, (2) purchase U.S.-origin goods (often energy or agricultural products), and/or (3) eliminate or adjust domestic regulations or policies viewed as impeding U.S. exports or business operations. In return, the Trump administration has offered reductions in country-specific IEEPA tariff rates and/or preferential treatment with respect to existing or forthcoming Section 232 tariffs.

Some agreements go beyond traditional market-access and investment commitments and include commitments to align with the United States on restrictions targeting third countries, including sanctions and export controls. For example, Cambodia appears to have agreed to take "similar measures" where the United States imposes sanctions or duties on a third country, while Malaysia agreed to adopt "measure[s] with equivalent restrictive effect."

The durability of these trade deals remains to be seen. With IEEPA-based tariffs acting as a primary negotiating point in these deals, a potential ruling by the Supreme Court striking down some or all of President Trump's IEEPA-based tariffs could motivate some U.S. counterparties to seek more favorable terms. Further, President Trump's tariff threats against European nations opposing his efforts to acquire Greenland called into question the future of the U.S.–EU trade deal, although the President has since walked back a tariff increase after reaching an apparent framework of a deal concerning use of the Danish overseas territory.

B. Uyghur Forced Labor Prevention Act

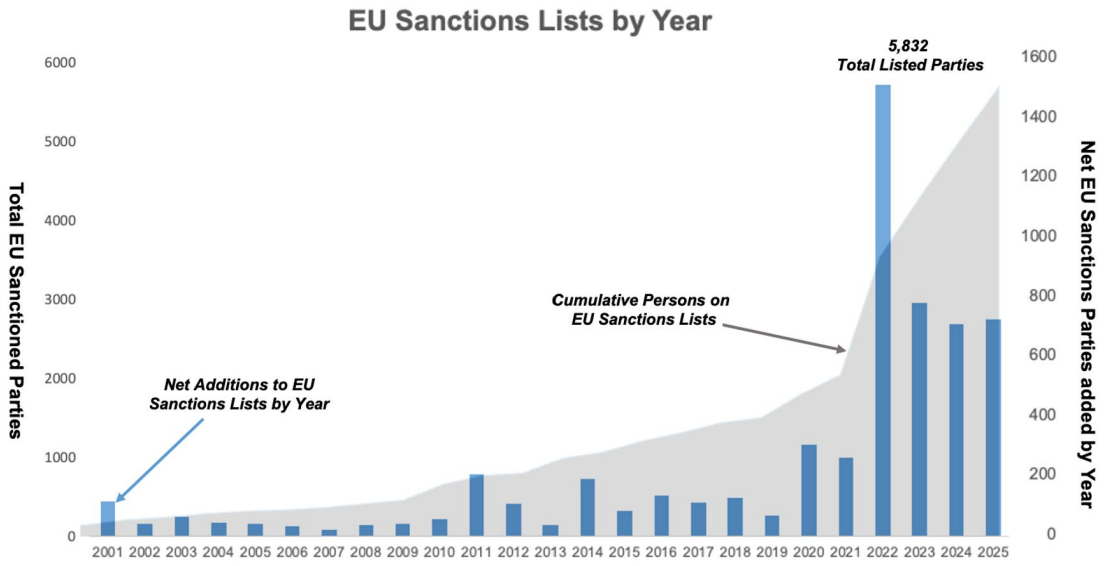
With tariffs taking precedence and U.S.–China trade relations stabilizing by mid-2025, CBP's enforcement of the Uyghur Forced Labor Prevention Act (UFLPA) has seemingly received less public attention and emphasis from the White House than in prior years. As discussed previously, the UFLPA—enacted with broad bipartisan support in 2021—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 prohibited from entry into the United States.

Notably, the outgoing Biden administration's addition of several dozen entities to the UFLPA Entity List in January was the only such expansion of that list in 2025. Still, under the second Trump administration, CBP's detentions under the UFLPA at U.S. ports have continued, with a particular focus on the automotive and aerospace industries. Moreover, in its annual strategy update report to Congress, DHS (in its role as chair of the interagency Forced Labor Enforcement Task Force) identified new "high-priority" sectors for enforcement, adding caustic soda, copper, jujubes, lithium, and steel to a list that already included aluminum, seafood, polyvinyl chloride, apparel, cotton and cotton products, silica-based products, and tomatoes.

Although the monetary value of goods detained under the UFLPA in 2025 was down from prior years, the most significant change in enforcement was the much lower percentage of detained shipments that were ultimately released. During fiscal years 2023 and 2024, approximately half of detained shipments were eventually released by CBP—apparently the result of successful "applicability review" submissions, a process whereby importers can seek the release of goods by demonstrating that they are not within the scope of the law's prohibitions (i.e., they were not produced in Xinjiang or by UFLPA Entity List parties). In fiscal year 2025, approximately 8 percent of detained shipments were released (592 released out of over 7,000 total shipments detained). As CBP continues to hone its expertise in targeting goods for detention under the UFLPA, importers face an uphill battle in challenging detention.

V. EUROPEAN UNION

A. Sanctions



1. Progress and Challenges in Harmonization

In 2025, sanctions policy confirmed its evolution from crisis instrument to a structural pillar of European Union strategy. The December 2025 Joint Communication by the European Parliament and the Council on Strengthening EU Economic Security made this shift explicit, positioning sanctions within a "proactive and systematic" framework to anticipate, deter, and respond to external threats. In Brussels' words, EU sanctions have moved "from a reactive posture towards a more proactive and systematic deployment of our toolbox."

The operational reality matched the rhetoric. The European Union's commitment to monthly rolling designations of Russia's shadow fleet vessels and their enabling ecosystem exemplified continuous pressure, rather than episodic crisis response. Simultaneously, the September 2025 Iran sanctions snapback demonstrated sanctions as an anticipatory instrument integrated within broader diplomatic and national security frameworks. This institutional maturation was also reflected by Brussels' integration of sanctions within a comprehensive economic security architecture spanning investment screening, export controls, and trade defense instruments.

Sanctions harmonization across the European Union remained a defining theme of 2025. In order to address long-standing disparities in Member State sanctions regimes, Directive (EU) 2024/1226 on the definition of criminal offenses and penalties for the violation of Union restrictive measures entered into force in May 2024. Sanctions enforcement in the European Union is done at the Member State level and consequently the Directive required Member States to incorporate its terms into national law by May 20, 2025. Crucially, the Directive establishes minimum rules criminalizing intentional sanctions violations and mandates maximum penalties of at least five years' imprisonment for natural persons and the higher of €40 million or 5 percent of total worldwide turnover for legal persons. Despite the May 20, 2025 deadline, as of late last year, 18

EU Member States—including major economies Germany, Spain, and France (which collectively account for nearly 50 percent of the bloc's gross domestic product)—had failed to adopt the measures into national law, prompting European Commission infringement procedures. However, the picture was not uniformly bleak: Sweden transposed the Directive, effective June 10, 2025, establishing imprisonment of two to six years for aggravated violations; the Netherlands notified existing legislative compliance; several Baltic and Nordic states demonstrated early adoption; Italy completed transposition on December 30, 2025, with Legislative Decree No. 211/2025 published in the Gazzetta Ufficiale on January 9, 2026, introducing new Criminal Code provisions that frame sanctions violations as crimes; and, in January 2026, the German government finally adopted the directive into domestic law (as discussed more fully below).

This disparity between EU Member States exposed tensions inherent in harmonization efforts. While the Directive provides common minimum standards for what conduct constitutes an offense and baseline penalties, critical implementation details—including the precise mental element required (e.g., intent, recklessness, negligence), procedural rules for investigation and prosecution, and evidentiary thresholds—remain governed by divergent national criminal law traditions. This means that even if all Member States had adopted the Directive, a transaction violating EU asset freeze obligations could face materially different treatment depending on the jurisdiction involved: what qualifies as "intentional" violation in one Member State's legal framework may differ from another's, and investigative tools available to prosecutors vary substantially across civil law and common law systems. Nevertheless, the Directive represents meaningful progress toward reducing forum shopping and regulatory arbitrage across the bloc. The establishment of minimum standards creates a baseline deterrent effect that, while imperfectly harmonized, marks significant evolution from the pre-2024 landscape where some EU Member States imposed only administrative fines (if that) for serious sanctions violations.

Enforcement activity intensified throughout 2025, but revealed persistent operational asymmetries across Member States, underscoring the challenge of translating unified policy into coordinated action. Finnish Customs reported initiating more than 900 investigations into sanctions violations since the start of the Ukraine war, with approximately 130 cases investigated as aggravated offenses—a dramatic increase from the two to ten regulatory offenses investigated annually before February 2022. Estonia's courts delivered multiple criminal convictions, with sentences ranging from suspended fines to five years' imprisonment, including convictions against companies and individuals for exporting luxury goods, dual-use items, and sanctioned products to Russia. Germany delivered notably severe custodial sentences, with a German court sentencing a businessman to five years in prison for arranging the export of 71 high-value vehicles to Russia through third countries to disguise their final destination, alongside asset seizures of approximately €5 million. Meanwhile, numerous EU Member States reported minimal or no public enforcement. These disparities reflect fundamental differences in enforcement architecture, prosecutorial priorities, resource allocation, investigative capacity, and, at times, political will, across the Union.

Against this fragmented backdrop, multilateral coordination mechanisms emerged as critical force multipliers. In November 2025, the European Anti-Fraud Office (OLAF) and Europol launched Project Transporter, a joint initiative targeting vehicle exports to third countries for possible onward transfer to Russia and Belarus. By combining Europol's analytical capabilities

(through its Target Group Sanctions unit) with OLAF's expertise in customs and EU expenditure fraud, the initiative provided coordinated support to Member States investigating sanctions breaches involving forged paperwork, complex diversion routes, and money laundering indicators. The partnership represents a recognition that commercially driven circumvention networks operating across multiple jurisdictions could not be effectively countered through isolated national enforcement alone. While enforcement statistics still show uneven commitment across the European Union, initiatives like Project Transporter signaled an institutional shift toward treating sanctions enforcement as a collective security imperative requiring integrated investigative efforts.

2. Russia

2025 marked a watershed in EU sanctions strategy against Russia. What began in February 2022 as reactive crisis management crystallized into the systematic deployment of economic restrictions. The four EU sanctions packages announced in 2025 reveal a deliberate escalation strategy: first broadening the net (16th package, in February), then sharpening anti-circumvention tools (17th package, in May), followed by direct targeting of key revenue sources (18th package, in July), and culminating in the financial targeting of Russia's largest oil companies (19th package, in October). This progression was carefully calibrated. Each package built on the weaknesses exposed by its predecessor, as Moscow's adaptive evasion tactics forced Brussels to shift from attacking Russian assets to dismantling the international ecosystem that enables their monetization.

The 16th package, unveiled on February 24, 2025 to mark the third anniversary of Russia's full-scale invasion of Ukraine, expanded traditional designations (48 individuals, 35 entities, 74 shadow fleet vessels, 8 media outlets, 13 financial institutions excluded from the Society for Worldwide Interbank Financial Telecommunication (SWIFT)) while establishing crucial regulatory architecture. Most significant was the extension of the "best efforts" obligation (which requires EU parent companies to ensure their foreign subsidiaries do not undermine sanctions) from trade restrictions under Council Regulation (EU) No 833/2014 to asset freezes under Council Regulation (EU) No 269/2014, demonstrating Brussels' focus on structural accountability mechanisms. The package extended transaction bans to enable listing of financial institutions and crypto asset providers participating in Russian oil price cap circumvention and facilitating transactions with shadow fleet vessels, directly targeting the payment infrastructure enabling evasion. Further, the European Union introduced a new designation criterion for individuals and entities that are part of Russia's military-industrial complex, support it, or benefit from it, broadening the net to the commercial ecosystem sustaining Russia's war effort. Previously, these companies could only be subject to stricter export restrictions (a tool the European Union continues to use extensively).

If the 16th sanctions package laid institutional groundwork, the 17th package (May 20, 2025) delivered an operational punch. Nearly 200 shadow fleet vessels were designated, more than doubling the total sanctioned tanker count and marking the most aggressive single-package targeting of Russia's maritime export infrastructure to date. The significance of this package, however, extended beyond vessel counts. By designating ***Surgutneftegas***, Russia's third-largest oil producer providing substantial government revenue, Brussels crossed a threshold it had carefully avoided for three years. The 17th package tightened the noose on Russia's

military-industrial supply chain by designating over 45 Russian companies providing drones, weapons, ammunition, and military equipment, plus, in a notable expansion, Chinese entities supplying machine tools to Russia's military and industrial sectors. This development underscored Brussels' willingness to impose costs on third-country enablers, not just Russian entities directly.

The shadow fleet campaign intensified further as the year progressed. By December 2025, the European Union had sanctioned an additional 50 vessels through rolling monthly designations, bringing the total to nearly 600, and shifted strategy from vessels alone to their enabling networks. Nine "shadow fleet enablers" (shipping companies in the United Arab Emirates, Vietnam, and Russia) were sanctioned in mid-December, followed by 41 more vessels days later. This pivot reflected hard-won operational insights. Sanctioning ships proved insufficient when new vessels could be rapidly recruited; dismantling the management, insurance, and brokerage networks proved far more effective.

The revenue impact validated the approach: EU data showed Russian oil revenues in March 2025 running 13.7 percent below March 2023 levels and 20.3 percent below March 2022. The 18th package (July 18, 2025) made the revenue pressure more acute by lowering the Russian crude oil price cap—the price of Russian-origin oil, above which certain services have been prohibited by the European Union, the United States, the United Kingdom, and other members of the Price Cap Coalition—from $60 to $47.60 per barrel and introducing a dynamic pricing mechanism designed to keep the cap below the average market price for Russian crude oil. The package simultaneously closed a crucial loophole by banning imports of petroleum products manufactured in third countries from Russian crude. Under customs rules, Russian crude exported to refineries in India, Turkey, and other non-sanctioning countries loses its Russian origin once substantially transformed into refined products. Previously, these products could then be legally reexported into EU markets, allowing Russia to monetize its crude indirectly, while third-country refineries captured the value-added margin. Early EU sanctions regulations, drafted with reference to customs principles, inadvertently created this easily exploitable gap. The new ban closed it by making the original Russian provenance of the crude determinative, regardless of where refining occurred. In line with Brussels' focus on the energy sector, the European Union additionally banned all transactions with the ***Nord Stream 1 and 2*** pipelines.

The 18th sanctions package also demonstrated Brussels' willingness to issue sanctions in ways very similar to OFAC's practice of designating actors for providing "material support" to sanctioned persons. The European Union imposed asset freezes on Russian and international ship managers, individual vessel captains, and operators of open flag registries, targeting actors throughout the shadow fleet value chain. Most notably, the package designated an Indian refinery majority-owned by Rosneft on grounds that it constituted a major Russian customer whose purchases sustained the shadow fleet's commercial viability. The European Union lacks OFAC's "material support" sanctions authority in the formal sense—that is, a designation basis in most U.S. Executive Orders that authorizes OFAC to sanction parties found to have provided material assistance or support to other sanctioned persons. However, these designations showed Brussels adopting a U.S.-style approach of targeting third-country entities whose

conduct, though not in violation of EU primary sanctions prohibitions, materially enables activities which do not align with EU foreign policy interests.

The 19th sanctions package (October 23, 2025) represented the year's culmination of trade restrictions against Moscow. Targeting Russian energy and finance with unprecedented directness, it imposed transaction bans on Rosneft and ***Gazprom Neft***, removing even the limited exemptions these major energy companies had previously enjoyed for certain products exported into the European Union. The package introduced a pathway toward a full Russian liquified natural gas (LNG) ban, sanctioned third-country entities facilitating circumvention, and significantly expanded restrictions on services provision to Russia. Perhaps most notably, it codified specific definitions for "ownership" and "control" concepts in Council Regulation (EU) No 269/2014, resolving years of interpretative ambiguity that had challenged compliance and enforcement. These definitions, which aligned with the non-legally binding EU Best Practices for Effective Implementation, provided welcomed legal clarity to regulators and the regulated across EU Member States.

By year end, the strategic sanctions calculus was clear: Russia faced a multi-pronged campaign targeting revenue generation (energy sector sanctions), transaction facilitation (shadow fleet elimination), financial system access (bank sanctions and services bans), and technology acquisition (export controls and catch-all provisions).

In parallel to sanctions escalation, the European Union advanced a broader policy effort to eliminate Russian energy dependence under the REPowerEU roadmap. The Commission's legislative proposal to phase out Russian LNG and pipeline gas imports—with full bans targeted for end-2026 and autumn 2027, respectively—represented a merger between sanctions policy and energy security strategy. The phasing process includes transition periods for existing supply contracts and mandatory national gas supply diversification plans, acknowledging that sanctions effectiveness requires viable alternative energy sources. This dual-track approach—punitive measures, combined with systemic restructuring—distinguishes the European Union's 2025 Russia strategy from the bloc's earlier attempts to pressure the Kremlin.

Another notable development saw Brussels do what the inter-governmental Financial Action Task Force (FATF) did not: add Russia to the European Union's own list of high-risk jurisdictions for money laundering and terrorist financing. The FATF—the global watchdog providing guidance and recommendations for combatting money laundering and terrorist finance—had suspended Russia's membership after the full-scale invasion of Ukraine but declined to blacklist it, prevented from doing so by opposition from the so-called BRICS countries—Brazil, Russia, India, China, and South Africa. The European Union's unilateral move hardwires Russia-related risks into European financial regulation, treating the Russian Federation not merely as a heavily sanctioned state but as a structural money laundering threat on par with Iran and North Korea. For EU regulated entities, the designation triggers mandatory enhanced due diligence on any relationship with a Russian nexus, which Brussels hopes that, for many market participants, will make Russian business too uneconomic and risky to retain.

3. Iran

The dominant development in EU–Iran sanctions was the September 2025 "snapback" of nuclear-related restrictions. On August 28, 2025, the E3 (France, Germany, and the United Kingdom) notified the UN Security Council that Iran was in "significant non-performance" of its JCPOA commitments, triggering a Security Council mechanism that, uniquely, operates without the opportunity for a veto by the Council's permanent members. On September 29, 2025, the European Union reimposed the full suite of EU nuclear-related economic and financial sanctions that had been lifted in 2016: bans on Iranian crude oil, natural gas, and petrochemical imports; prohibitions on energy sector equipment and technology transfers; asset freezes on the Central Bank of Iran and major Iranian financial institutions; and restrictions on specialized financial messaging services. The snapback transformed the Iran compliance landscape overnight, requiring companies with any Iranian exposure to reassess counterparties, supply chains, and contractual obligations against a sanctions framework not seen since before the JCPOA's implementation.

Parallel to the nuclear regime, the European Union continued to renew the implementation of its dedicated framework targeting Iran's UAV and missile programs. Currently listing a range of individuals and entities—including drone component manufacturers, propellant producers, shipping companies, the Islamic Revolutionary Guard Corps Navy, Islamic Republic of Iran Shipping Lines, Iranian airlines, and Iran's Defense Minister and Deputy Minister—the regime reflects the evolution of EU–Iran sanctions beyond their traditional nuclear focus. New designations have targeted transnational procurement networks supplying UAV components to Russia and armed groups destabilizing the Middle East and Red Sea region, while export bans now prohibit EU transfers of components used in drone and missile development to Iran.

As outlined in our detailed alert, the reinstatement of the European Union's nuclear-related sanctions did not trigger any amendment to Council Regulation (EC) No 2271/96 (the EU Blocking Statute). EU operators therefore remain prohibited from complying with certain extraterritorial U.S. sanctions targeting Iran that conflict with EU measures. In practice, however, the Blocking Statute's relevance in the Iran context has diminished following the reimposition of substantive EU sanctions on Iran.

Early actions in January 2026 signal continued pressure on Iran, as the European Council announced additional human rights-related designations in response to Tehran's violent repression of peaceful protests, and further sanctions targeting Iran's UAV program to counter Iranian military support to Russia. In a notable shift, the European Union also decided to list the Islamic Revolutionary Guard Corps as a terrorist organization.

4. Syria

The past year delivered an unexpected sanctions pivot on Syria. Following the sudden collapse of the Assad regime in December 2024 and the establishment of a transitional authority, the European Union suspended, and ultimately lifted, its Syria sanctions regime to facilitate humanitarian access and economic reconstruction. This shift represented a cautious policy bet: working in accord with similar U.S. sanctions relief (discussed above), Brussels sought to support Syria's transition while retaining the ability to reimpose measures if the security situation

deteriorates or designated individuals from the previous regime resurface in positions of influence.

EU asset freezes on designated individuals and entities were lifted, trade restrictions on oil, luxury goods, and controlled items were suspended, and sectoral restrictions on finance, transport, and telecommunications were removed. However, the underlying legal framework remains in place, allowing rapid reimposition if conditions warrant. Indeed, the European Union characterized its actions with respect to Syria as reversible, if necessary.

Crucially, as with the U.S. relief, certain sanctions and export control measures remain in place, such as those targeting the Assad regime, chemical weapons, and illicit drug trade, as well as a number of sectoral measures relating to arms, dual-use goods, equipment for internal repression, software for interception and surveillance, and the import and export of Syrian cultural heritage goods. In light of the security risks involved, it is unlikely that the European Union will lift these measures in the near future.

5. Case Law and Referrals to the CJEU

The rapid succession of the European Union's Russia sanctions packages in 2025, in addition to new measures responding to geopolitical tensions, has created a highly complex legal landscape, susceptible to interpretative divergence and fraught with compliance and implementation challenges. Consequently, 2025 saw an unprecedented rise in referrals from national courts of EU Member States to the Court of Justice of the European Union (CJEU).

a) Interpretation of "Freezing of Funds" in Russia Regulations

In response to a Dutch Supreme Court request for a preliminary ruling, in C-465/24, the Advocate General of the CJEU addressed a question with significant practical implications: whether "freezing of funds" within the meaning of EU asset freeze legislation extends to voting rights attached to securities, or applies only to monetary transactions. The Advocate General advised the CJEU that "freezing of funds" should be interpreted broadly to encompass voting rights and meeting participation. Permitting sanctioned persons to exercise corporate governance rights would enable them to influence decisions affecting the economic value of their holdings, an outcome incompatible with the sanctions regime's objectives. If the CJEU follows this opinion, the court would unequivocally confirm the long-held position in practice that asset freezes neutralize not just a sanctioned party's ability to transact, but also their capacity to exert corporate influence.

Although not binding, Advocate General opinions carry significant persuasive authority and frequently shape the development of EU law. The CJEU's eventual judgment, expected in early 2026, could bring the European Union into line with U.S. interpretations of the prohibitions that accompany asset freeze measures.

b) Asset Freeze Measures and Trusts

In C-483/23, the Advocate General provided an opinion clarifying how Article 2(1) of Council Regulation (EU) No 269/2014 applies to assets held in trusts established by sanctioned persons. The case, referred by the Regional Administrative Court of Lazio, Italy, concerned a Bermuda trust whose settlor had been designated under EU sanctions. The opinion confirms that substance prevails over form: even where legal title has passed to a trustee, a sanctioned settlor may still be deemed to "own, hold, or control" trust assets for sanctions purposes if they retain significant powers, such as the ability to revoke the trust, appoint or remove trustees, or influence distributions to beneficiaries. The opinion is very similar to a recent line of OFAC enforcement cases concerning continued sanctioned-party control over trusts nominally held by non-sanctioned parties.

Although non-binding, the Advocate General opinion signals increased scrutiny of trust structures used by sanctioned individuals, particularly offshore trusts with flexible terms that preserve settlor influence. It aligns with the purposive interpretation adopted by the English Commercial Court in ***EuroChem v. Société Générale*** (discussed below), reinforcing that sanctions compliance requires looking beyond formal legal arrangements to the underlying reality of control.

c) Interpretation of "Control"

In C-84/24, the Supreme Court of Lithuania referred to the CJEU questions concerning whether a 50 percent shareholding by a designated person creates a presumption that the company's assets are "controlled" within the meaning of Article 2(1) of Council Regulation (EC) No 765/2006, the Belarus Sanctions Regulation. Advocate General Ćapeta advised that, while the asset freeze does not automatically extend to non-listed companies, a 50 percent shareholding creates a rebuttable presumption of control over that company's funds and economic resources, obliging banks to freeze immediately while preserving the company's right to challenge.

Critically, the Advocate General distinguished the Article 2(1) freezing obligation from the Article 2(2) prohibition on making funds available: these are "autonomous and distinct" measures, meaning a company cannot rebut the presumption of control merely by showing its assets are not used "for the benefit of" the designated shareholder. Factors such as separation of company and shareholder assets, management by non-designated persons, and/or restricted account access may be relevant but are individually insufficient to overcome the presumption. The opinion confirms that "control" in sanctions law differs from corporate law; the question is not whether the designated person can freely dispose of assets, but whether they can influence how the company's funds are used.

d) Interpretation of "Acting on Behalf or at the Direction of"

In C-313/24, the Council of State (Italy) referred a question concerning whether Article 5k(1)(c) of Council Regulation (EU) No 833/2014—which prohibits awarding public contracts to persons "acting on behalf or at the direction of" Russian nationals or Russian-established entities—applies where two of three board members of an Italian company are Russian nationals, one of whom serves as chairman, chief executive officer, and sole director of the 90 percent-owning parent company. Advocate General Spielmann advised that the prohibition does not apply

automatically based solely on the Russian nationality of company directors. Rather, the concept of "acting on behalf or at the direction of" requires a substantive, fact-specific assessment of whether the tenderer is under the *de facto* control of Russian nationals or entities. While the presence of Russian nationals in key management positions is not determinative, such circumstances, particularly nationality combined with roles, ownership links, and governance responsibilities, "may serve as relevant indicators requiring further scrutiny by the contracting authority."

The Advocate General emphasized that the relevance of a director's nationality should be limited to scenarios where the director holds powers beyond day-to-day management, exercising strategic decision-making authority or control over the company's broader objectives. The assessment should consider all relevant circumstances, including the role and influence of the ultimate beneficial owner. The Advocate General left it to the referring court to determine whether such an assessment is required in the specific case. Although that opinion arises in the public procurement context, its reasoning has broader significance: the phrase "acting on behalf or at the direction of" appears throughout the EU sanctions framework—including in the transaction ban—and the emphasis on substance over form suggests that authorities and operators must look beyond corporate formalities to assess whether *de facto* control exists whenever that formulation is invoked.

e) Exception Mechanism under the EU Blocking Statute

In Case T-518/23, the General Court addressed the Commission's power to grant retroactive authorizations under the EU Blocking Statute. The Blocking Statute generally prohibits EU operators from adjusting their conduct to comply with, or avoid the consequences threatened by, specified extraterritorial U.S. sanctions measures, but the Commission may grant an exception where it would seriously harm the interests of the operator or the European Union.

An Iranian bank on the U.S. SDN List challenged European Commission decisions granting ***Clearstream Banking AG*** an exception to the Blocking Statute to freeze the Iranian bank's securities in order to avoid exposure to U.S. sanctions-related risks. The Court confirmed that, while retroactive effect is exceptional, such authorizations may be granted retroactively where two conditions are satisfied: the purpose to be achieved so demands, and the legitimate expectations of those concerned are duly respected. The General Court rejected the argument that the Commission's Guidance Note precluded retroactivity. The judgment—only the second substantive General Court ruling on the Blocking Statute after ***IFIC Holding***, and the third major EU court decision on that subject, following the CJEU's 2021 ruling in ***Bank Melli Iran***—confirms that the exception mechanism in the legislation is a flexible tool capable of accommodating the practical realities of protracted administrative procedures, while reaffirming that third parties targeted by U.S. sanctions enjoy no procedural rights under the Blocking Statute framework.

6. Member State Perspective: Germany

Germany has cemented its position as the European Union's most zealous enforcer of sanctions. With over one hundred Public Prosecutor's Offices pursuing cases, criminal enforcement has surged following Russia's full-scale invasion of Ukraine, and shows no signs of slowing.

The scale of activity is striking. In April and September 2025, Germany's Federal Economic Ministry (formerly *Bundesministerium für Wirtschaft und Klimaschutz*, and now rebranded as *Bundesministerium für Wirtschaft und Energie*) (BMWE) published two official digests cataloging criminal enforcement actions tied to Russia sanctions. Four cases stood out: courts handed down multi-year prison sentences for covertly supplying sanctioned goods to Russia, often using circuitous routes via Hong Kong, Kyrgyzstan, Kazakhstan, the United Arab Emirates, Turkey, Switzerland, Lithuania, and Belarus. The contraband ranged from electronic components for use in drones, to dual-use machine tools for use by an arms manufacturer, to passenger cars. Asset confiscations in these cases ran from €880,000 to €30 million. Customs offices from Berlin to Stuttgart and prosecutors in Munich are reportedly pursuing dozens more investigations into similar export violations and illicit imports of Russian caviar substitutes.

German regulators have been busy issuing guidance to match. BMWE updated its Russia sanctions FAQs and published new guidance targeting circumvention schemes involving computer-programmed milling machines and lathes. Germany's Federal Office for Economic Affairs and Export Controls (*Bundesamt für Wirtschaft und Ausfuhrkontrolle*) (BAFA) refreshed its Russia trade leaflet and added new circumvention-prevention materials. The German Federal Bank (*Deutsche Bundesbank*) updated its FAQs on EU financial sanctions, while the domestic intelligence service (*Bundesamt für Verfassungsschutz*) (BfV), released an information sheet on procurement tactics used by state actors to evade both proliferation controls and sanctions.

When the European Union triggered the snapback of EU nuclear-related sanctions on Iran in late September 2025, German agencies moved swiftly. BAFA overhauled its Iran trade guidance, covering both the restored restrictions and its general licensing framework. The Bundesbank published guidance on the authorization procedure for Iran-related transfers of funds restricted under the restored EU sanctions regime, as well as its authorization and notification forms related to this procedure.

BAFA also continued issuing general licenses (i.e., regulatory carve-outs within the EU sanctions framework). In July 2025, it extended General License No. 42 until March 2027, permitting eligible parties to provide otherwise-restricted services and software to non-sensitive Russian recipients, such as EU subsidiaries. In December 2025, it reissued General License No. 30, adapting it to the restored Iran sanctions but declining, for now, to extend its validity beyond March 2026.

Meanwhile, Germany's sanctions criminal law has undergone its most significant overhaul in years. Although Berlin initially missed the May 2025 deadline to adopt EU Directive 2024/1226 into German law, prompting the European Commission to open infringement proceedings, the new government led by Chancellor Friedrich Merz ultimately revived the legislation, which the Bundestag passed in January 2026.

This reform sharpens the law's teeth considerably. The reform amends the core criminal and administrative offense provisions of Sections 18 and 19 of the Foreign Trade and Payments Act (*Außenwirtschaftsgesetz*) (AWG) and Section 82 of the Foreign Trade and Payments Ordinance (Außenwirtschaftsverordnung) (AWV). Conduct previously punishable only as administrative infractions now constitutes a criminal offense under German law if committed intentionally. Even negligent violations involving dual-use items can be qualified as a crime if reckless. Practically any breach of EU sanctions may now warrant a German criminal investigation. While Germany did not link statutory fines for companies to global turnover, it quadrupled the maximum fixed fine amount contemplated by the Directive from €10 million to €40 million. New offenses target circumvention tactics, including asset concealment through third parties, and a fresh provision in the Residence Act (*Aufenthaltsgesetz*) criminalizes facilitating sanctioned persons' entry into the country. German prosecutors were already aggressive; the tightened framework will only intensify their efforts.

As part of the same legislative package, Germany also introduced a new instrument of public fiduciary administration under Sections 6a through 6f of AWG. The provision authorizes the BMWE to place EU-based subsidiaries of certain designated Russian entities under a public trusteeship to the extent required to avert a threat to public order or security. The appointed trustee may assume control over the company by exercising shareholder rights and taking the measures necessary to ensure the continued lawful operation of the business. According to the legislative materials, the instrument is intended to enable the continued participation of affected EU subsidiaries in economic activity while ensuring compliance with the EU sanctions.

Looking ahead, the coalition agreement of the new government, which took office in May 2025, signals a broader overhaul of German foreign trade law. Export licensing is expected to be streamlined and accelerated, with comprehensive prior checks giving way to targeted, random inspections backed by stiff penalties. Within the scope of this system, the need for individual licensing may be reduced significantly. Yet, the coalition agreement also emphasizes that rigorous enforcement of Russia-related sanctions will continue unabated.

B. Export Controls

The European Commission's and High Representative's 2025 Joint Communication to the European Parliament and the Council on the European Economic Security Strategy confirmed export controls' position alongside sanctions and investment screening as core tools for protecting European national security interests, including technological sovereignty. In recent years, EU institutions have been reflecting on the effectiveness of current tools, and the European Commission's January 2024 White Paper on export controls had identified areas for improvement.

This past year, the European Union took tangible steps in the direction of increasing the impact of these controls. The European Union maintains a centralized regime governing the export of dual-use goods through Regulation (EU) 2021/821, which directly applies across all Member States and aligns with multilateral agreements to which EU Member States are party, most notably the Wassenaar Arrangement. Historically, this multilateral framework ensured that European controls kept pace with technological developments through consensus-based updates to control lists agreed at annual Wassenaar plenary meetings. That mechanism has broken down since Russia's full-scale invasion of Ukraine, as Russia, like any other Wassenaar member, holds veto power over any initiative to amend the control lists and used it to block the adoption of important controls on emerging technologies. This dysfunction prompted several EU Member States—including the Netherlands, Germany, Italy, France, and Finland—to adopt unilateral controls, giving rise to a complex compliance patchwork across the European Union.

To address this fragmentation, in 2025 the European Commission took the unprecedented step of independently adding controls for technologies not regulated at the multilateral level. The updated EU control list adds new categories, including quantum technology and quantum computers, semiconductor manufacturing and testing equipment, advanced computing integrated circuits, additive manufacturing machines and related materials, and peptide synthesizers. In April 2025, the European Commission also issued a Recommendation aimed at enhancing coordination of national control lists of dual-use items, which was a key focus of the Commission's January 2024 White Paper on export controls. The Recommendation introduces a coordination mechanism, which allows Member States to share draft lists with the Commission and other Member States, inviting feedback before their formal adoption, and foreshadowing potential future EU-wide controls where national divergence proves untenable.

C. Foreign Direct Investment

Five years after the European Union established a cooperation mechanism for investment screening, the system's limitations have become as visible as its achievements. National regimes now cover nearly all EU Member States, but divergent rules and procedures persist, prompting a reform agreement in December 2025 aimed at greater harmonization.

In December 2025, representatives of the European Council and the European Parliament reached a provisional political agreement on the revision of the foreign direct investment (FDI) screening regulation, with application expected approximately 18 months after entry into force. The revisions strengthen the current system, mandating screening mechanisms to be carried out by all Member States, and covering foreign investments through EU subsidiaries as well. The reform introduces a harmonized minimum scope covering defined sensitive areas (including dual-use items, critical raw materials, hyper-critical technologies such as AI, quantum and semiconductors, and specific categories of financial service providers), mandatory prior authorization for investments in these areas, strengthened cooperation obligations between Member States, and streamlined procedures with standardized two-phase review and aligned definitions. EU institutions are also considering the introduction of a power to screen unnotified transactions retroactively. If adopted, the reform will require all Member States to update their FDI screening regimes and will result in more rigorous scrutiny, tighter timelines, and enhanced EU-level coordination.

The agreement comes as the European Commission's fifth annual report on the application of the EU Foreign Direct Investment Screening Regulation, published in October 2025 and covering data gathered in 2024, reveals both the regime's growing maturity and the continued fragmentation it seeks to address. The European Union saw a continued slowdown in FDI inflows in 2024, with an 8.4 percent decline, following a 23 percent drop in 2023. The decrease was driven primarily by a 19 percent fall in greenfield investments, while M&A activity experienced a modest year-on-year recovery of 2.7 percent. The United States and the United Kingdom remained the largest sources of foreign investment into the European Union, together accounting for approximately 60 percent of both M&A and greenfield activity. Within the Union, Germany was the preferred destination for M&A transactions (21 percent), while Spain received the most greenfield investments (24 percent).

Despite the decline in inflows, screening activity across Member States continued to intensify. In 2024, EU Member States notified 477 investments to the European Union's cooperation mechanism, broadly in line with the 488 notifications in 2023. The number of notifications to the EU cooperation mechanism has increased by 15 percent since 2021, a sign of maturation. Most cases (92 percent) were closed within two weeks, with only eight percent requiring an in-depth security risk assessment. The Commission issued opinions in less than two percent of cases. At the national level, the vast majority of screened investments (86 percent) were cleared unconditionally, with only nine percent cleared subject to conditions and one percent ultimately blocked (and the remaining four percent of filings were withdrawn by the parties before a formal decision was made), confirming that while screening volumes are rising, the proportion of investments identified as posing serious security concerns remains low. Sectors triggering the largest share of notifications remained consistent with previous years: manufacturing, information and communications technology, wholesale and retail, financial activities, and professional services. The most common ultimate origin of investors remained the United States and the United Kingdom, while the share of transactions involving Chinese ultimate investors rose from six percent in 2023 to nine percent in 2024.

Across the European Union, many Member States maintained stable frameworks while others introduced targeted amendments. France revised its list of critical research and development technologies, Lithuania expanded its regime to cover crypto assets, and Sweden broadened the scope of "essential services" into the digital sphere. Energy infrastructure, particularly offshore wind, faced increased scrutiny. Other reforms focused on coordination and transparency, including enhanced cooperation between screening and competition authorities (Czechia), mandatory digital filings (Germany), and expanded public reporting practices.

All 27 EU Member States have now enacted FDI screening regimes, although those in Croatia and Cyprus are not yet fully operational. Croatia's regime, adopted under a designation-based model, will require authorities to identify "obliged entities" by April 2026, while Cyprus's regime will enter into force in April 2026 for non-European Economic Area (i.e., outside of the European Union, Iceland, Liechtenstein, and Norway) and non-Swiss investments in sensitive sectors.

VI. UNITED KINGDOM

A. Sanctions

The United Kingdom's National Security Strategy 2025, published in June, positions economic statecraft—sanctions, export controls, and investment screening—as central to protecting British interests in an era of heightened geopolitical competition. The December 2025 Anti-Corruption Strategy extends this logic further, deploying sanctions not merely to constrain adversaries but to dismantle kleptocratic networks and the professional enablers who service them. Much as with the European Union, the message is clear: sanctions are no longer a reactive diplomatic instrument but a proactive tool of state power.

The past year's developments reflected this duality of policy aggression and institutional build-out. UK sanctions designation volumes remained high, with continued pressure on Russia, expanded measures against Iran following the JCPOA snapback, and a new standalone sanctions regime targeting irregular migration. UK sanctions enforcement matured in parallel. The Office of Trade Sanctions Implementation (OTSI) completed its first full year of operation, while the Office of Financial Sanctions Implementation (OFSI) launched a comprehensive consultation proposing substantial penalty increases and procedural reforms, signaling that implementation firepower is finally catching up with policymakers' ambitions.

Coordination with UK allies has deepened despite broader strains on multilateralism. An OFAC-OFSI Memorandum of Understanding, published in January 2025, formalizes information-sharing arrangements that had operated informally since Russia's invasion of Ukraine. Visiting officers from OFSI and OFAC now walk each other's halls, and joint designations with Washington, including coordinated action against Gazprom Neft and Surgutneftegas, and continued alignment with EU and Group of Seven (G7) partners on initiatives such as the Russian oil price cap, demonstrate that London remains committed to collective economic pressure even as transatlantic relations face new uncertainties. The United Kingdom also sought to extend its reach beyond formal alliances: the Foreign, Commonwealth & Development Office published guidance specifically aimed at non-UK businesses operating in third countries, outlining circumvention risks and practical compliance steps—a clear signal that the United Kingdom (like the United States) expects its sanctions to cast a long shadow beyond its own jurisdiction.

Domestically, UK sanctions enforcement has become embedded in a whole-of-government economic crime framework. The Economic Plan 2: System Priorities – 2025 coordinates efforts across OFSI, the National Crime Agency (NCA), and other enforcement bodies, while OFSI's increasingly intelligence-led approach (supported by over 210 international engagements across 44 jurisdictions in 2024-25) suggests a regulator moving from passive compliance monitoring toward active threat disruption.

1. Russia

The United Kingdom's Russia sanctions strategy in 2025 moved decisively from incrementalism to escalation, marked by three inflection points that fundamentally reshaped the compliance landscape. First, the designation of Russia's energy giants Rosneft and Lukoil—a week ahead of OFAC's parallel designations to the SDN List—ended years of calculated restraint on oil

majors, signaling that no Russian company, regardless of revenue contribution or market significance, remained too systemically important to sanction. Second, the reduction of the oil price cap from $60 to $47.60 per barrel represented the sharpest single adjustment since the cap's introduction, deliberately squeezing Russia's export margins. Third, the sustained monthly designations of shadow fleet participants, that by October 2025 exceeded 500 vessels, demonstrated the United Kingdom's commitment to systematically dismantling Russia's maritime export infrastructure.

What emerged was not simply "more sanctions," but an overarching theory of economic pressure: constrict revenue at the source (oil company sanctions), raise transaction costs (price cap reduction), and systematically dismantle enabling infrastructure (targeting the shadow fleet and the surrounding maritime ecosystem, such as ship owners and managers). The operational tempo reinforced these themes. Major packages in February (marking the invasion's third anniversary with 67 individuals, entities, and 40 shadow fleet vessels), May (a wide-ranging package targeting military operations, energy exports, weapons supply chains, and 46 financial institutions), and rolling monthly shadow fleet additions created continuous pressure designed to close gaps exposed by Moscow's previous evasion attempts.

The cumulative impact by year-end was substantial: 1,816 individuals, 562 entities, and more than 500 shadow fleet vessels sanctioned under the United Kingdom's Russia regime alone, with £28.7 billion in Russian-linked assets frozen since February 2022. These figures are notable not only in volume but also in strategic coverage: the individual designations target beneficial owners and facilitators; the entity designations covered energy, finance, military-industrial, and circumvention nodes; and the vessel designations aimed to make Russian oil exports increasingly expensive and difficult to insure and transport.

Direct vessel designations, an authority only introduced in July 2024, became a core enforcement tool during 2025, bringing the UK regime into closer alignment with U.S. practice and demonstrating London's willingness to move aggressively against maritime infrastructure. The United Kingdom's November 2025 issuance of a "Red Alert" on Russia's shadow fleet codified the compliance expectations accompanying this designation surge. The alert highlighted specific typologies warranting enhanced due diligence: Automatic Identification System manipulation, opaque ownership and management structures, ship-to-ship transfers, frequent flag changes, and irregular insurance arrangements. These were not mere risk indicators but actionable red flags requiring escalation from maritime, insurance, finance, and logistics actors.

The technology and software controls introduced in April 2025 represented a crucial new development in UK Russia sanctions. The measures, which operate independently from the software's export control classification, target business enterprise, industrial design, and oil and gas-related software, and expand technology transfer restrictions. The restrictions are supported by new OTSI guidance clarifying scope, compliance expectations, and license application requirements. The General Trade License (Russia Sanctions – Sectoral Software and Technology) provides a limited pathway for certain legacy contractual obligations, subject to eligibility verification, condition compliance, and registration.

Finally, circumvention risk remained top of mind for UK policymakers throughout 2025. OTSI's business guidance detailed practical steps to identify and mitigate evasion—including third-country routing, intermediary chains, complex ownership structures, and "no-Russia" clause diversions—thereby helping develop a benchmark for risk-based compliance design. The NCA's "Operation Destabilise" publicly connected Russian-linked money-laundering networks to drugs, ransomware, and hostile-state activity, highlighting how sanctions evasion increasingly embeds within broader criminal ecosystems. For businesses, this points toward greater convergence of sanctions compliance, anti-money laundering controls, and cyber incident response. Enhanced beneficial ownership diligence, controls on crypto exposure, clear red-flag escalation, and coordinated cross-functional case management are emerging as best practices for managing risk effectively, particularly in higher-risk corridors or where opaque payment and logistics structures are involved.

2. Iran

UK policy toward Iran in 2025 reflected a strategic hardening across multiple fronts. Parliament's Intelligence and Security Committee published an impactful report characterizing Iran as a "wide-ranging, persistent and sophisticated threat" to UK national security, concluding that Iranian state threat activity had been historically under-recognized and that the physical threat to UK-based dissidents was now comparable to that posed by Russia. The government responded by placing Iran (alongside Russia) on the enhanced tier of the Foreign Influence Registration Scheme, requiring anyone directed by the Iranian state to conduct activities in the United Kingdom to register or face imprisonment.

The sanctions response was equally muscular. Following the UN sanctions snapback, the United Kingdom reinstated its pre-JCPOA sanctions framework, reactivating expansive restrictions across petroleum, petrochemicals, shipping, financial services, and industrial sectors. The United Kingdom went further, and designated an additional 71 individuals and entities beyond those caught by the snapback, targeting procurement networks, front companies, and facilitators supporting Iran's nuclear program and regional military activities. London's approach reflects several strategic calculations: maintaining pressure on Iran's nuclear program while preserving space for future diplomacy; targeting drone and missile capabilities flowing to Moscow and Tehran's regional proxies, thereby connecting Iran sanctions to broader Russia and Middle East policy; and closing gaps in previous iterations of its sanctions regime.

The legislative toolkit expanded in parallel. The Independent Reviewer of Terrorism and State Threat Legislation published recommendations in May 2025 supporting the introduction of bespoke tools to address hostile state activity falling short of traditional terrorism, including sanctions-like mechanisms for state-linked entities, which the UK government led by Prime Minister Keir Starmer has committed to develop. The National Security Act 2023 also received its first Iran-related test when three Iranian nationals were charged with offenses relating to surveillance targeting UK-based journalists, prompting the summoning of the Iranian ambassador. Parliamentary debate revealed broad cross-party consensus supporting the government's layered approach combining sanctions, criminal enforcement, and counter-state-threat legislation.

The cumulative effect is a UK posture toward Iran that now operates across multiple vectors simultaneously—sanctions, criminal enforcement, counter-state-threat legislation, and registration requirements—with broad political consensus behind further escalation. The direction of travel points toward continued tightening, particularly if Iranian domestic instability or regional confrontation intensifies.

3. Syria

The United Kingdom followed Brussels and Washington in lifting a substantial portion of its Syria sanctions following the Assad regime's collapse. Amendments to the UK Syria sanctions regulations announced in April 2025 removed restrictions across Syria's finance, banking, energy, and transport sectors, enabling the country to reconnect to the SWIFT messaging system in June after decades of exclusion and to export oil for the first time in 14 years. In October 2025, the government removed Hay'at Tahrir al-Sham from the list of proscribed terrorist organizations under the Terrorism Act 2000, enabling closer engagement with President Ahmed al-Sharaa's fledgling government. With the World Bank estimating reconstruction costs at over $216 billion, the United Kingdom has positioned Syria as a "potentially high return market" despite its challenging context, issuing new industry guidance in December 2025 to support commercial engagement.

Notwithstanding these developments, significant UK prohibitions remain in force. Measures targeting Assad-era actors, chemical weapons, dual-use and military goods, goods used for internal repression, interception and monitoring software, and the import and export of gold, precious metals, diamonds, and luxury goods continue to apply. Asset freezes remain in place against approximately 350 Syrian individuals and entities. The United Kingdom has also made clear it will continue to deploy targeted sanctions against Syria-related parties responsible for repression and human rights abuses: in December 2025, six individuals and three organizations were designated in connection with the March coastal violence in Latakia and Tartous and Assad-era atrocities. Engagements involving Syria should therefore continue to be subjected to scrutiny, as sanctions relief has opened commercial pathways, but not all UK restrictions have been lifted.

4. Enforcement Trends

a) Recent OFSI Actions

UK sanctions enforcement in 2025 marked a turning point. OFSI imposed four monetary penalties, more than in any previous year and more than half its cumulative total since acquiring penalty powers in 2017. The message is clear: the era of cautionary letters is ending.

A £300,000 penalty against ***Markom Management Limited*** (Markom) (a UK-based financial services company) set the tone. Beyond the substantial penalty amount for a single violative transaction, the action is noteworthy as the conduct at issue occurred under pre-Brexit sanctions regulations, demonstrating OFSI's willingness to pursue historic breaches rather than confine enforcement efforts to recent violations. Aggravating factors included Markom's alleged absence of sanctions controls for informal intra-group transactions and an eight-month delay before

disclosure. Governance shortcomings and slow engagement now function as penalty multipliers, and the passage of time offers no safe harbor.

In a rare action against a sophisticated player, the global law firm ***Herbert Smith Freehills*** was fined £465,000 for payments made by its former Moscow office to sanctioned Russian banks during a hasty wind-down in May 2022. OFSI also imposed a £152,750 penalty on ***Colorcon Limited*** (Colorcon) (the UK subsidiary of a global pharmaceutical company) for similar failures involving its Moscow representative office, reinforcing that even exiting from heavily sanctioned jurisdictions can carry substantial compliance risks. The Colorcon case is also noteworthy because the company's voluntary disclosure discount was reduced from 50 to 35 percent due to a four-month delay between discovering the breaches and notifying OFSI, a surprising outcome given the time and resource commitment required to adequately investigate and document compliance shortcomings.

Two further actions underscored OFSI's expanding enforcement toolkit. A £5,000 penalty against ***Svarog Shipping & Trading Company Limited***—OFSI's first enforcement action based solely on an "information" offense (i.e., failing to respond to an OFSI request for information)—signaled that procedural non-compliance and poor engagement with regulators can, in themselves, trigger penalties. By contrast, a disclosure notice (but no monetary penalty) issued to ***Vanquis Bank Limited*** for an eight-day delay in freezing a designated person's account demonstrated that a timely voluntary self-disclosure and cooperative engagement can materially mitigate consequences.

The direction of travel for OFSI sanctions enforcement is unmistakable: greater frequency, broader sectoral reach, and a willingness to penalize process failures, not just substantive breaches.

b) FCA Sanctions Enforcement and Implementation

The UK Financial Conduct Authority's (FCA) £29 million fine against *Starling Bank* in October 2024 cast a long shadow over 2025 and crystallized the FCA's enforcement philosophy on sanctions. The regulator's focus is not on policies as written but on controls as operated, including: data quality, timely identification and interdiction of matches; documented scenario coverage for higher-risk products and corridors; testing regimes; governance that challenges performance rather than rubber-stamps it; and clear, well-documented escalation and remediation where potential breaches are identified. The FCA's evolving enforcement posture, with higher fines and a streamlined enforcement pipeline, indicated lower tolerance for weaknesses in first- and second-line ownership of sanctions risk, with expectations that firms could demonstrate effective adaptation to frequent designation updates, complex ownership/control analyses, and evolving circumvention typologies.

In line with its wider financial crime mandate, the FCA conducted 266 sanctions compliance assessments in 2024-2025, with particular attention to payments and trade finance touchpoints where circumvention risk is highest. The FCA's 2025 supervisory work remained tightly focused on whether firms' sanctions screening and associated governance functioned effectively in practice, with particular attention to data quality, model calibration, testing, and assurance. While cross-government coordination on sanctions evolved over the year, the FCA's lens remained

supervisory: translating external typologies and intelligence into testing of firms' end-to-end controls and ensuring timely remediation where weaknesses were identified.

Supervisory testing through 2025 concentrated on higher-risk products and corridors, including payments and trade finance touchpoints, where robust end-to-end screening, counterparty diligence, and alert handling were expected to promptly detect and interdict sanctions exposure. As circumvention typologies evolved, the FCA increasingly scrutinized firms' risk assessments, data lineage, model risk management, and the responsiveness of tuning and triage to frequent designation changes.

Looking ahead to 2026, firms should expect continued, data-led scrutiny of screening calibration and governance, increased use of multi-firm reviews and skilled-person work where systemic issues persist, and sustained testing of end-to-end sanctions controls across payments, trade finance, and higher-risk correspondent relationships. The FCA is also likely to maintain focus on third-country circumvention risks and rigorous escalation and disclosure practices where potential breaches are identified.

c) The Maturing UK Enforcement Landscape: HMRC, OFSI, and OTSI

Three developments in 2025 signaled ongoing structural shifts in UK sanctions enforcement: the emergence of a criminal pipeline, a proposed overhaul of civil penalties, and the operationalization of a new trade sanctions authority.

In February 2025, His Majesty's Revenue and Customs (HMRC) provided a rare quantitative snapshot of its enforcement operations to the Treasury Select Committee: it reported 30 live criminal investigations into potential sanctions offenses, up from zero in 2021, with 27 of those inquiries relating to Russia. HMRC has recruited 40 additional investigators, enhanced overseas intelligence gathering, and formalized an enforcement partnership with the newly established OTSI under which serious civil cases are referred for criminal consideration. Six compound settlements (i.e., civil penalties) totaling £1.36 million have been concluded for Russia-related trade sanctions breaches, including the largest single penalty of £1.16 million in May 2025. The practical implication is that self-disclosure and engagement decisions must now account for a more mature UK enforcement landscape, featuring cross-referrals between civil and criminal pathways.

In parallel, OFSI's 2025 consultation on civil enforcement reform signals a material elevation in UK financial sanctions risk. As set out in a prior client alert, the proposals include:

- Increasing statutory maximum penalties from £1 million or 50 percent of breach value, to £2 million or 100 percent;
- Capping voluntary disclosure discounts at 30 percent (down from 50 percent) and tightening eligibility criteria;
- Introducing a formal settlement scheme modelled on the Prudential Regulation Authority's approach;

- Creating an "Early Account Scheme" to expedite investigations in exchange for enhanced discounts; and
- Streamlining penalties for information, licensing, and reporting breaches.

2025 marked the end of OTSI's inaugural year as the dedicated UK civil enforcement authority for trade sanctions. The figures in OTSI's "One Year" update reflect a regime in build-out mode: 60 license applications received (predominantly Russia-related professional and business services); over 140 suspected breach reports triaged for investigation, referral to HMRC, or information-sharing with international partners; and no civil monetary penalties yet imposed, presumably a function of phased prioritization rather than enforcement appetite. Looking ahead, OTSI has signaled a shift toward more proactive use of its civil powers, expansion of its licensing remit, and more detailed guidance on breach reporting, the license application process, and compliance expectations.

The cumulative effect is a UK enforcement system that now operates across financial sanctions (OFSI), trade sanctions (OTSI and HMRC), and regulated-firm supervision (FCA)—with increasingly formalized civil-criminal escalation processes.

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) Contractual Performance and U.S. Sanctions Risks

In ***Ceto Shipping Corporation v. Savory Shipping Inc***, the Commercial Court considered when a party may refuse contractual performance on sanctions grounds under a "reasonable judgment" clause. The Court confirmed that such clauses do not require proof that performance would *certainly* result in sanctions; a serious possibility of exposure suffices. The judgment must be made in good faith and be objectively reasonable, but the process of reaching it need not be optimal; what matters is whether the conclusion was reasonable, not whether the enquiries were exhaustive.

Importantly, sanctions risk is assessed prospectively: the absence of prior designations against comparable actors does not preclude a reasonable judgment that risk exists, particularly where enforcement priorities are evolving. The Court also held that where two sanctions risks intersect (here, Iranian-origin cargo destined for Venezuela) the combined effect may intensify the overall risk, even if neither alone would be determinative. For parties operating in sanctions-sensitive trades, the decision confirms that a well-founded risk assessment, grounded in market intelligence and contemporaneous enforcement trends, can justify non-performance even without formal legal advice, provided the judgment is genuine and objectively defensible.

The judgment is also notable for its treatment of U.S. sanctions risk in an English law context. The vessel, its owners, and its managers had no connections to the United States, and the proposed voyage would not have violated UK sanctions law. Nevertheless, the Court accepted that the risk of being designated to the U.S. SDN List, and the catastrophic commercial consequences that would follow, was a legitimate basis for invoking the contractual protection. The Court preferred the evidence of Savory Shipping's expert, who testified that the risk of designation was "high" given OFAC's enforcement priorities during the relevant period, over that of Ceto Shipping's expert, who characterized the risk as "low" based on the absence of prior designations against comparable European operators. In reaching that conclusion, the Court emphasized that U.S. secondary sanctions operate by threatening designation rather than direct prohibition, and that English courts will give weight to a party's reasonable assessment of that threat when considering whether contractual non-performance was justified. The practical implication is significant: a party to an English law contract may lawfully decline to perform where it reasonably judges that performance would expose it to U.S. secondary sanctions, even if performance would be lawful under English and EU law.

b) Ownership and Control in the Context of Trust Structures

LLC EuroChem North-West-2 v. Société Générale is the most significant English court decision to date on the application of Council Regulation (EU) No 269/2014's asset freeze measures to complex corporate and trust structures. The claimants, Russian subsidiaries of the *EuroChem* fertilizer group, sought payment under English law for on-demand bonds totaling over €280 million. The issuing banks refused payment on the grounds that the claimants were owned or controlled by a designated person, such that the bonds were frozen and payment was prohibited. The Court dismissed the claims.

On ownership, the Court held that a beneficiary under a discretionary trust is to be treated as the owner of the trust assets for the purposes of Council Regulation (EU) No 269/2014, even though a discretionary beneficiary has no proprietary interest under English or Bermudian trust law. The regulation must be given an autonomous, purposive interpretation; domestic trust law concepts are not determinative. The Court further held that the trust in question was not a "true" discretionary trust because its terms allowed the designated person to retain effective control (here, through his ability to secure the appointment of a trusted deputy as protector, with powers to remove trustees and influence decision-making).

On control, the Court confirmed that *de facto* control is sufficient. No legal relationship between the designated person and the entity is required. A person may be said to control an entity where they are able to influence its decisions, even in the absence of any legal tie, ownership link, or equity participation. Evidence that employees continued to regard the designated person as "the man at the top," and that corporate decisions were made by reference to the designated person's wishes, was sufficient to establish control, notwithstanding formal structural changes made after designation. The Court also emphasized that where a designated person's spouse was appointed as successor beneficiary of a discretionary trust immediately upon designation, the Court would scrutinize whether they were acting as a mere proxy, particularly where a trusted deputy of the designated person was simultaneously appointed as protector.

The judgment is notable for its treatment of corporate firewalls as a mechanism for entities to escape the reach of Article 2 of Council Regulation (EU) No 269/2014. The Court accepted that the Swiss parent company had implemented effective firewall measures which satisfied the relevant national competent authorities—in Switzerland, France, Cyprus, and the Netherlands—that it was no longer subject to an asset freeze. However, the Court held that firewalls protect only the entity that implements them and its EU subsidiaries: subsidiaries outside the European Union that have not implemented equivalent measures remain frozen, even if their parent has been released. As the French national competent authority (the *Direction Générale du Trésor*) made clear, "in the absence of an adequate measure to verify the activities of subsidiaries established outside the European Union, these remain subject to the asset freezing measures."

The Court also held that a determination by a national competent authority that an entity is owned or controlled by a designated person is determinative for purposes of the domestic law of that Member State. Where such a determination has been made, an English court will treat the question of ownership or control as settled for the purposes of assessing foreign illegality, rather than conducting its own independent assessment. This has significant implications for the enforcement of English law obligations where performance would occur in an EU Member State.

c) Illegality and the UK Blocking Regulation

Beneathco DMCC v. R.J. O'Brien Limited provides important guidance on the interaction between the *Ralli Brothers* principle and U.S. sanctions, and on the scope of the UK Blocking Regulation (the UK equivalent of the EU Blocking Statute, discussed above). The *Ralli Brothers* principle provides that a contract governed by English law is unenforceable insofar as performance would require an act to be done in a place where that act would be unlawful.

The claimant, a Dubai company designated by OFAC as an SDN, sought payment of approximately $16.5 million held for it by a UK broker. The Court held that the claimant's payment instructions were not ones with which the broker was contractually obliged to comply, because the contract required payment in U.S. dollars to the claimant itself, whereas the instructions sought payment in a different currency or to a third party. In the alternative, the Court held that even if such an obligation existed, it would be suspended by the *Ralli Brothers* principle. On the evidence, any transfer of U.S. dollars from the broker's UK banks to Dubai would necessarily involve U.S. correspondent banks, and the use of such banks to effect payment to a designated person would be prohibited under U.S. law. The Court confirmed that the *Ralli Brothers* principle extends to unlawful acts by third parties, such as correspondent banks, where those acts form part of contractually required performance, not merely preparatory steps.

The claimant argued that the UK Blocking Regulation precluded reliance on the *Ralli Brothers* principle, on the basis that compliance with OFAC's prohibitions would itself be a criminal offense under UK law. The Court rejected this argument. It held that the UK Blocking Regulation targets only the extraterritorial application of the listed U.S. laws—it does not apply where the relevant unlawful conduct (here, the correspondent bank's participation in the transfer) would occur *within* U.S. territory. Moreover, the relevant provisions of the Executive Order under

which the claimant was designated derived from IEEPA, which is not among the statutes listed in the annex to the UK Blocking Regulation.

B. Export Controls

1. UK Accedes to the Agreement on Defence Export Controls

The United Kingdom's accession to the Agreement on Defence Export Control (ADEC) in December 2025—joining France, Germany, and Spain—marks another significant step in British defense export policy, complementing the AUKUS export control exemptions that took effect in September 2024. While AUKUS eliminated licensing requirements for the vast majority of defense trade with Australia and the United States, the ADEC addresses a different challenge: the procedural friction that has historically complicated multinational defense programs with tightly integrated European supply chains. For qualifying collaborative programs, ADEC streamlines licensing through enhanced inter-authority consultation. Where supply chain transactions involve less than 20 percent of the value of components from another signatory, export authorizations are to be issued "without delay."

Crucially, the ADEC does not override international obligations or relax substantive controls. The UK Export Control Act 2002 and the Strategic Export Licensing Criteria remain fully applicable, and the Export Control Joint Unit (ECJU) will continue to assess each license application on its merits. What the treaty provides is procedural alignment, reducing administrative friction while leaving the underlying legal requirements intact. The ECJU has indicated that implementing guidance and an open general export license (OGEL) to support the treaty will follow in due course.

2. Regulatory Amendments and Licensing

The Export Control (Amendment) (No. 2) Regulations 2025 removed the United Kingdom's standalone national controls on sensitive emerging technologies (control entries PL9013, 9014, and 9015) from Schedule 3 of the Export Control Order 2008 and incorporated them into the assimilated Dual-Use Regulation as new "500 series" entries. This mirrors the EU amendments that took effect in November 2025 and ensures that UK controls on quantum computing, semiconductor manufacturing equipment, and advanced materials remain current and interoperable with both EU and U.S. regimes, while avoiding regulatory divergence between Great Britain and Northern Ireland. The amendments also update the assimilated Torture Goods Regulation and revise Schedule 4 to reflect the lifting of the UK arms embargo on Armenia and Azerbaijan (while retaining transit controls). As the ECJU has revised relevant OGELs, companies should reassess eligibility and update screening tools accordingly.

The ECJU's licensing statistics for the second quarter of 2025 underscore the increasing complexity of the UK export control environment. License refusals remain elevated, exceeding 100 per quarter consistently since the third quarter of 2022, well above the long-term quarterly average of 77. China continues to account for the majority of refusals, driven predominantly by the military end-use controls introduced in recent years and the addition of China to the list of destinations subject to those controls. Processing times have been affected by a combination of

factors: the transition from the legacy SPIRE system to the new LITE platform, the expanding scope of sanctions measures, and the growing complexity of dual-use casework.

3. Enforcement Trends

HMRC's export control enforcement in 2025 showed increased activity, though the United Kingdom continues to lag behind the United States in the scale and visibility of its export enforcement actions.

In the first quarter of 2025, HMRC concluded compound settlements totaling £3.7 million with three exporters for unlicensed exports of military-listed goods under the Export Control Order 2008, including a single settlement of £3.2 million. These did not relate to sanctions offenses. In May 2025, HMRC concluded its largest-ever compound settlement for a Russia sanctions breach: a £1.16 million fine for making goods available to Russia in violation of the Russia (Sanctions) (EU Exit) Regulations 2019. A further £620,000 settlement followed in September 2025 for unlicensed exports of military goods.

Compound settlements are typically offered where a breach appears inadvertent or stems from control weaknesses and the exporter has voluntarily disclosed the issue. HMRC generally withholds the identities of businesses found in violation, which limits the market's ability to derive detailed compliance lessons from individual cases. Even so, the available data reinforces the value of prompt voluntary disclosure and demonstrable remediation, particularly given the cross-referral pathway now established between OTSI (for civil trade sanctions) and HMRC (for criminal consideration of serious cases).

The increase in maximum summary fines, while modest in absolute terms, signals a clearer policy intent to make a wider range of export control offenses (particularly those involving brokering, technical assistance, and intangible transfers) more readily prosecutable. The direction of travel is toward greater enforcement activity, even if the United Kingdom has not yet matched the frequency or transparency of U.S. actions by BIS and its sister agencies.

C. Foreign Direct Investment

The UK National Security and Investment Act 2021 (NSI Act) remained in active operation in 2025, with notification volumes continuing to rise. During the reporting period from April 2024 to March 2025, the Investment Security Unit (ISU) received 1,143 notifications—over 25 percent more than the prior year—though the regime continued to quickly clear the vast majority of transactions: 95.5 percent were approved at Phase 1, with only 4.5 percent called in for in-depth review. Final orders were issued in just 17 cases, of which 16 involved the imposition of conditions and only one required divestment. This low intervention rate confirms that the NSI Act operates as a targeted filter rather than a barrier to investment in the United Kingdom.

That said, increased volumes have modestly affected processing times. It now takes a median of seven working days to accept a mandatory notification (up from six) and 20 days to reject a notification (up from 13). Defense-related transactions continued to predominate, accounting for 56 percent of all notifications and 36 percent of call-ins. Notably, the regime remains nationality-agnostic in design: among called-in transactions, 48 percent involved UK acquirers, 32 percent

Chinese, and 20 percent American, reinforcing that scrutiny turns principally on the target's activities within the NSI Act's sensitive sectors, rather than the acquirer's national origin.

In parallel, the UK government launched a consultation, which closed in October 2025, proposing the first significant amendments to the Notifiable Acquisition Regulations since 2022. The proposals would create three new standalone sectors (critical minerals, semiconductors, and water), while narrowing others, such as AI (to exclude low-risk internal use of consumer tools) and data infrastructure (to focus on third-party data centers). The government has also announced an intention to exclude purely internal corporate reorganizations and the appointment of insolvency practitioners from mandatory notification, though no draft legislation has yet been published. On the government's estimates, the net impact would be modest, ranging from 10 fewer to 35 additional notifications per year, but the reforms signal a maturing regime calibrated to reduce compliance burdens while focusing resources on transactions that present genuine national security risks.

2025 also brought important legal precedent in FDI screening. In ***R (FTDI Holding Limited) v. Chancellor of the Duchy of Lancaster*** (*FTDI*), the High Court in July 2025 upheld a final order requiring divestment of an 80.2 percent stake in a UK semiconductor business acquired by Chinese-backed investors before the NSI Act came into force. The Court confirmed that "awareness" for the purposes of the six-month call-in clock is not limited to the relevant minister but can be met by ISU staff, a finding that provides useful clarity on when time begins to run. On proportionality, the Court conducted its own assessment but afforded a high degree of deference to the government's evaluation of national security risks, accepting that the Secretary of State's view on what measures were necessary and proportionate was entitled to "great respect." The Court further held that procedural shortcomings, including insufficient reasoning in the final order itself, were not sufficient to invalidate the order where the decision-maker was found to have had good reasons for the decision.

This judicial deference was reinforced by the Court of Appeal in ***L1T FM Holdings v. Chancellor of the Duchy of Lancaster*** (*LetterOne*), which dismissed a challenge to the lack of compensation following a compelled divestment. The Court held that there is no absolute right to "fair market value" compensation under Article 1 of the First Protocol to the European Convention on Human Rights. Where the investor conducted a sale in the open market, selected a buyer subject only to national security suitability, and retained the proceeds, this satisfied the requisite "reasonable relationship of proportionality," even though timing and compulsion affected bargaining dynamics.

The combined effect of *FTDI* and *LetterOne* is to confirm that, while judicial review remains available, UK courts will afford substantial deference to the executive on national security matters. Investors should note that national security measures can result in financial losses without compensation even where, as the Court of Appeal observed, "there is no suggestion that the investor entities have done anything wrong." Outside the courtroom, the *Versarien Plc* prohibition in August 2025, blocking the transfer of graphene-related intellectual property and know-how to a proposed joint venture with China's *Anhui Boundary Innovative Materials Technology*, served as a reminder that the NSI Act captures not only share acquisitions but also asset transactions, including intangible know-how, licensing arrangements, and collaboration

access. Where dual-use technology is at stake, structuring a transaction as a joint venture or technical-assistance arrangement will not avoid scrutiny.

* * *

The second Trump administration entered office with a clear vision that the tools of international trade—tariffs, sanctions, export and investment controls—can be used to further a wide range of the White House's foreign policy, national security, and domestic economic goals. The result has been an unprecedented application of these tools, which has been met by judicial challenges in the United States and an increasingly robust response from the European Union, the United Kingdom, China, and others—all of whom have increasingly resorted to similar old and novel instruments as they have pursued and protected their own interests.

For companies on the front lines of these trade wars, 2025 was an introduction to a new, highly complex, fluid, and increasingly disaggregated trading and regulatory landscape. Even so, if one steps back from the day-to-day noise and discerns the broader policy interests that are animating so many states to pursue their interests via coercive economic measures, opportunities may emerge.

Please click on the link below to view the complete update and endnotes on Gibson Dunn's website:

Read More

The following Gibson Dunn lawyers prepared this update: Anna Searcey, Irene Polieri, Adam M. Smith, Stephenie Gosnell Handler, Christopher T. Timura, Matthew S. Axelrod, Ronald Kirk, Donald Harrison, Benno Schwarz, David Wolber, Claire Shepherd, Alana Tinkler, Attila Borsos, Michelle Kirschner, Samantha Sewall, Roxana Akbari, Jason Bae, Karsten Ball, Dharak Bhavsar, Sarah Burns, Soo-Min Chae, Alex Chiang, Justin duRivage, Hui Fang, Erika Suh Holmberg, Janice Jiang, Neringa Juodkunaite, Saad Khan, Zach Kosbie, Maria Kosmopoulou, Josephine Kroneberger, Melina Kronester, Vanessa Ludwig, Nikita Malevanny, Dorkas Medina, Chris Mullen, Mason Pazhwak, Nick Rawlinson, Layla Reynolds*, Dominic Solari, Audi Syarief, Scott Toussaint, 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 Advisory & Enforcement or Sanctions & Export Enforcement practice groups:

United States:

Adam M. Smith – Co-Chair, Washington, D.C. (+1 202.887.3547, asmith@gibsondunn.com)
Ronald Kirk – Co-Chair, Dallas (+1 214.698.3295, rkirk@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)
Matthew S. Axelrod – Washington, D.C. (+1 202.955.8517, maxelrod@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)
Roxana Akbari – Orange County (+1 949.475.4650, rakbari@gibsondunn.com)
Karsten Ball – Washington, D.C. (+1 202.777.9341, kball@gibsondunn.com)
Sarah Burns – Washington, D.C. (+1 202.777.9320, sburns@gibsondunn.com)
Hugh N. Danilack – Washington, D.C. (+1 202.777.9536, hdanilack@gibsondunn.com)
Justin duRivage – Palo Alto (+1 650.849.5323, jdurivage@gibsondunn.com)
Zach Kosbie – Washington, D.C. (+1 202.777.9425, zkosbie@gibsondunn.com)
Dorkas Laura Medina – Washington, D.C. (+1 202.777.9444, dmedina@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)
Erika Suh Holmberg – Washington, D.C. (+1 202.777.9539, eholmberg@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 – Singapore (+65 6507 3692, fxue@gibsondunn.com)
Qi Yue – Beijing (+86 10 6502 8534, qyue@gibsondunn.com)
Dharak Bhavsar – Hong Kong (+852 2214 3755, dbhavsar@gibsondunn.com)
Soo-Min Chae – Singapore (+65 6507 3632, schae@gibsondunn.com)
Hui Fang – Hong Kong (+852 2214 3805, hfang@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)

**A recent law graduate who is not admitted to practice law.*