FOLEY HOAG WHITE PAPER

Review of International Trade Enforcement in the U.S., E.U., and UK in 2024 and What to Expect in 2025

MARCH 2025

FOLEY HOAG

www.foleyhoag.com

TABLE OF CONTENTS

INTRODUCTION

Throughout 2024, enforcement of international trade laws continued to gather pace while the primary targets of enforcement were familiar ones: China, Russia, and Iran. Numerous agencies issued enforcement regulations and guidance. For example, the U.S. Department of Justice's ("DOJ") National Security Division ("NSD") announced an updated enforcement policy, the U.S. Department of Commerce Bureau of Industry and Security ("BIS") updated regulations related to voluntary disclosures and issued guidance aimed at academic institutions and financial institutions, and the Department of the Treasury's ("Treasury") Office of Foreign Assets Control ("OFAC") released guidance and an interim final rule related to its extended statute of limitations and recordkeeping requirements. With the new administration in the U.S., however, there appear to be new priorities. On one hand, the Trump administration may use sanctions and export controls as a tool to broker a resolution to Russia's war on Ukraine. If successful, however, we could see a rapid reduction in enforcement with respect to Russia-related actions. In the interim, a previously unified Western position on Russia is fracturing, increasing the prospect that enforcement risks for companies operating in Russia will be greater under EU and UK laws than under U.S. law. On the other hand, as described below, the Trump administration has shown signs that it intends to more closely focus on China and Iran—which could result in potential increased enforcement related to those jurisdictions.

Initial indications also clearly demonstrate that the Trump administration is less concerned with holding U.S. companies accountable for violations of international trade laws. As a result, the enforcement environment for non-U.S. companies may be more challenging than for U.S. companies. This is particularly true for companies in jurisdictions that the Trump administration targets for trade-related countermeasures (such as tariffs).

On the EU side, the EU is likely to stay focused on steadily and consistently applying sanctions against Russia, as it did throughout 2024. But the intensity may depend on each Member State's respective approach to Russian sanctions—given some tend to be more aggressive in this regard than others. Nonetheless, the UK is likely to continue working closely with the EU on its efforts to sanction Russia. The UK will also likely try to keep coordinating with U.S. agencies, such as OFAC, to enforce international trade regulations.

THE U.S. ENFORCEMENT LANDSCAPE

I. March 2024 Tri-Seal Compliance Note

On March 6, 2024, the DOJ, BIS, and OFAC announced their first—and only—Tri-Seal Compliance Note of 2024 (the "March 2024 Note"). The March 2024 Note concerns the applicability of U.S. sanctions and export controls to non-U.S. individuals or entities located in foreign countries or territories. describes the available range of enforcement mechanisms

to hold non-U.S. persons accountable, including criminal prosecution. It provides illustrative examples of the type of conduct where OFAC would seek to penalize foreign persons including, for instance, a scenario in which a non-U.S. person conducts an illicit transaction using the U.S. financial system. The March 2024 Note also describes the broad reach of BIS' enforcement power, noting "U.S. export control laws may extend to items subject to the EAR anywhere in the world and to foreign persons who deal with them."

II. U.S. Export Controls Enforcement Updates

Along with the March 2024 Note, BIS issued guidance on multiple occasions throughout 2024, while bringing several notable enforcement actions.

A. BIS Enforcement Guidance and Announcements

1. Guidance Regarding Different Types of BIS Letters

On July 10, 2024, BIS released industry guidance explaining the differences between three types of letters is has issued, namely, "red flag," "supplier list," and "is informed" letters ("BIS Industry Guidance"). As noted in BIS' Export Enforcement: 2024 Year in Review, BIS sent over 40 such letters in 2024. According to BIS:

- "Supplier list" letters identify non-U.S. persons who raise foreign policy or national security concerns but are not found on BIS' public screening lists. The recipient of a supplier list letter may or may not have dealt with any of the named persons. The intent of this letter is to put the recipient on notice that the named persons may present a compliance risk and therefore merit additional scrutiny.

- "Red flag" letters are specific warnings that the named persons (identified as customers of the recipient) may have violated the EAR by reexporting or transferring (in-country) the same kind of item that the recipient previously exported to that customer. These letters specifically instruct recipients to conduct additional due diligence to resolve the red flag before filling any order from that customer.

- "Is informed" letters are notifications to the recipient of applicable license requirements based on U.S. foreign policy or national security concerns. These letters put the recipient on notice that engaging in a transaction described in the "is informed" letter without obtaining the necessary license would violate the EAR.

2. BIS Compliance Note and Compendium of Resources for Academic Institutions

On August 14, 2024, BIS published a Compliance Note: Trends in Voluntary Self-Disclosures Related to Academia to Inform Improvements to Export Compliance Plans ("Compliance

Note to Academia"). Its purpose was to identify commonly disclosed violations and describe steps to take to avoid such violations. The most common violations include:

- Exports of microorganisms, chemicals, and toxins, including small amounts (or vials) of biological agents (e.g., Dengue-2 virus)—in violation of BIS export controls.
- Unauthorized exports to persons on the Entity List.
- Failure to file required Electronic Export Information in BIS's Automated Export System and undervaluing items connected to the export transaction(s).

BIS explained that most violations stem from an academic institution's lack of familiarity with, or misunderstanding of, the relevant export regulations, and that the primary way to avoid such violations is by enhancing the institution's compliance program, including with export controls training.

Alongside the Compliance Note to Academia, BIS released a compendium of resources for academic institutions. BIS presented this as a comprehensive guide to export compliance, providing links to the consolidated screening list and a BIS webpage describing how to develop an export compliance program.

3. BIS Final Rule on VSD Process and Penalty Guidelines

BIS issued its final rule on the Voluntary Self-Disclosure Process and Penalty Guidelines, on September 12, 2024 (the "VSD Rule") to enhance the voluntary self-disclosure process and update the penalty guidelines for administrative enforcement cases. The rule introduces a dual-track system for handling VSDs, distinguishing between minor or technical violations and significant violations. Minor or technical violations can now be disclosed through an abbreviated narrative report, which can be bundled and submitted quarterly, while significant violations require a more detailed narrative. The VSD Rule emphasizes that a deliberate decision not to disclose a significant apparent violation will be considered an aggravating factor in determining penalties, which raises the question of whether BIS is essentially imposing a mandatory disclosure regime. The VSD Rule also expands the scope of past corporate criminal resolutions that OEE may consider when determining enforcement. This factor now includes not only where a respondent has been convicted or entered a guilty plea, but also where a party has entered into any other type of resolution with DOJ or other authorities, including a Deferred Prosecution Agreement or a Non-Prosecution Agreement.

The updated penalty guidelines reflect changes to how BIS calculates penalties, particularly by removing base penalties for non-egregious cases and instead tying penalties to the transaction value. According to BIS, this change addresses scenarios where previous guidelines resulted in disproportionately low penalties that failed to serve as effective deterrents. The VSD Rule also eliminates specific percentage ranges for reductions

associated with certain mitigating factors, allowing for a more flexible and case-specific approach to penalty determination. Additionally, the rule formalizes non-monetary penalties, such as suspended denial orders with compliance conditions, as a response to non-egregious violations that do not result in serious national security harm. The VSD Rule also removes from the Penalty Guidelines all specific percentage ranges for potential penalty reduction based on various mitigating factors. In doing so, "OEE is making clear that the civil monetary penalty will be adjusted (up or down) to reflect the applicable factors for administrative action set forth in the BIS Penalty Guidelines." The VSD Rules also adds a new aggravating factor for transactions that enable human rights abuses.

The VSD Rule incorporates several policy changes announced in BIS memoranda since 2022, aimed at strengthening the administrative enforcement program and encouraging VSDs. In addition to the changes highlighted above, the VSD Rule clarifies that any person, not just the person who committed the violation, may notify BIS's Office of Export Enforcement ("OEE") that a violation has occurred and seek a waiver of General Prohibition 10 ("G10"). The VSD Rule also codifies the concept that disclosure of conduct by others that leads to an enforcement action counts as "exceptional cooperation." BIS will provide cooperation credit for such tips in "a future enforcement action, even for unrelated conduct" to the party submitting the disclosure. However, the VSD Rule provides no details on how the credit will be applied.

On the same day the VSD Rule was issued, BIS appointed its first-ever Chief of Corporate Enforcement, Raj Parekh. In this role, he advances corporate investigations by serving as the main interface between BIS' agents, the DOJ, and the Department of Commerce's Office of Chief Counsel for Industry and Security. However, the Trump administration disbanded the Corporate Enforcement Unit within DOJ's National Security Division ("NSD") on February 5, 2024, raising questions about how long Mr. Parekh's position will remain.

4. BIS Financial Institution Guidance

On October 9, 2024, BIS provided "New Guidance to Financial Institutions on Best Practices for Compliance with the Export Administration Regulations" ("Financial Institution Guidance"), describing best practices that financial institutions "should adopt in order to minimize their risks of violating the EAR, including" G10.

For instance, BIS advises financial institutions to screen clients against BIS restricted party lists and cross-check customers—and, as needed, the customers of those customers—against lists of entities that have shipped items appearing on the Common High Priority List to Russia since 2023 based on "publicly available trade data." Such items include, for example, electronic integrated circuits and products used to create semiconductors. BIS explains that it does not expect financial institutions to screen parties to every transaction in real time for the sake of preventing G10 violations. However, BIS does recommend, in

situations involving transactions that have a high probability of being connected to exports from the U.S. or in-country transfers or reexports outside the U.S. (e.g., those entailing cross-border payments), that financial institutions screen against certain specified lists (e.g., the Unverified List, Entity List, Military End-User List, and Denied Persons List).

5. *BIS' Updated "Don't Let This Happen to You" Guidance*

BIS announced an updated version of its "Don't Let This Happen to You" guidance, on November 12, 2024. In this publication, BIS describes its fiscal year 2024 enforcement activity that "led to the criminal conviction of over 65 individuals and businesses for export violations with penalties of nearly $5 million in criminal fines, nearly $3 million in forfeitures, over $15 million in restitution and over 3,100 months of imprisonment."

B. BIS Export Controls Enforcement Actions

While there was no BIS enforcement action in 2024 as significant as the $300 million penalty imposed on Seagate Technology LLC in 2023, the enforcement actions described below are notable.

1. *Unauthorized Shipments to Russia or China*

With respect to Russia, the following enforcement actions stand out:

- June 13, 2024: BIS brought an enforcement action against an aviation company headquartered in Turkey, Sapphire Havacilik San Ltd. STI ("Sapphire"). BIS imposed a $285,000 penalty on Sapphire because it flew its Russian national client (who was using a Cyprus passport), via a privately chartered Gulfstream aircraft originating in the U.S., into Russia.

- December 18, 2024: BIS settled with Integra Technologies, Inc. ("Integra"), a California-based engineering and manufacturing company. BIS imposed a $3.3 million penalty based on Integra shipping—without obtaining the required authorizations—numerous products used for radar systems or avionics (e.g., transistors) to Russian end users, from February to October 2023. Some shipments occurred after the products in question had been designated as CHPL items. Integra knew the items were going to Russian-end users, but its compliance systems failed to account for February 2023 EAR updates prohibiting the export of such items without the required license.

- December 23, 2024: BIS entered a settlement with the Indium Corporation of America ("Indium"), a New York entity that manufactures and supplies materials to thermal management, electronics, semiconductor, and thin-film markets. BIS imposed a $180,000 mitigated penalty based on solder products Indium exported to Russia from April 2022 to March 2023. While these are nominally EAR99 items, the exported

goods were classified under Harmonized Tariff Schedule codes requiring Indium to obtain a license.

As to China, on November 1, 2024, BIS agreed to a $500,000 settlement with GlobalFoundries U.S. Inc. and its subsidiary ("GlobalFoundries"). GlobalFoundries shipped $17.1 million of semiconductor wafers to a China-based company included on the Entity List, SJ Semiconductor ("SJS"), without obtaining the required license. Though SJS was a third-party outsource assembly and test service provider, instead of its customer, BIS noted GlobalFoundries had a duty to make sure its compliance system picked up SJS' involvement. Due to a data input error, however, GlobalFoundries failed to properly screen SJS. This action shows why U.S. persons exporting to China need to carefully screen their counterparties (and end users) to ensure they are not transacting with persons on the Entity List.

Most recently, on January 17, 2025, BIS, together with OFAC, required California-based Haas Automation, Inc. ("Haas"), to pay a combined civil penalty of $2.5 million. According to BIS, Haas engaged in illicit exports of Computer Numerical Control machine parts to Russian and Chinese persons on the Entity List.

2. *BIS Imposed Previously-Suspended Denial Order on Forwarder for Violating Settlement Terms*

On June 17, 2024, BIS imposed a denial order against USGoBuy LLC ("USGoBuy"), a package forwarding company based in Oregon, restricting its export privileges for three years, because of persistent EAR violations and the failure to address previous compliance errors. In 2021, USGoBuy, had entered a settlement with BIS that provided for a suspended penalty in the form of a three-year denial order—which BIS could implement if USGoBuy engaged in post-settlement EAR violations or otherwise violated the terms of the settlement. USGoBuy conducted an audit (required by the 2021 settlement) that identified numerous export violations USGoBuy had failed to address. Homeland Security Investigations then intercepted a package containing an export-controlled item headed to USGoBuy's warehouse and ultimately destined for China. Homeland Security placed explicit labels on the intercepted package explaining that an export license was required to ship it and released the package to be delivered to the USGoBuy warehouse. USGoBuy then proceeded to export the package the same day without the required license in violation of the EAR. Based on these violations, BIS imposed the previously-suspended penalty.

This enforcement action shows that those who enter into settlements with BIS that contain suspended penalties, particularly export denial orders, should carefully comply with such agreements or risk losing their export privileges altogether.

3. BIS Administrative Enforcement Activity

A few administrative penalties BIS imposed in 2024 are noteworthy. First, on February 12, 2024, BIS announced its intent to bring an administrative proceeding against New York-based Cargosave Inc. ("Cargosave"). In two instances, between September and December 2016, Cargosave violated the EAR by facilitating shipments of switches and enterprise servers from the U.S. to Iran, without the requisite export licenses. Consequently, Cargosave agreed to (1) a suspended denial of its export privileges for two years and (2) provide an EAR compliance training program to the relevant employees.

Second, on June 24, 2024, BIS released an order imposing administrative penalties on Indiana University for its alleged exports of a certain species of genetically modified fruit flies without the necessary license. Indiana University was not required to pay a monetary penalty but agreed to a suspended denial of its export privileges for one year. Assistant Secretary for Export Enforcement, Matthew Axelrod, noted that the penalty was meant to serve as a message to research institutions to strengthen their export compliance programs.

Finally, on September 30, 2024, a Texas company, First Call International Inc. ("First Call") entered an administrative settlement with BIS for almost $440,000 (suspended in part). According to BIS, First Call filed a backdated document with BIS, making it appear as if its transaction complied with the EAR, and it separately engaged in exports of military parts without proper authorization. First Call presented the falsified document to BIS in response to a BIS request for a copy of a Prior Consignee Statement, which exporters need to obtain before they can take advantage of License Exception Strategic Trade Authorization. First Call did not have the document, so it attempted to deceive BIS by asking its non-U.S. customer to back-date it.

4. List-Based Enforcement Actions

BIS added a significant number of companies to the Entity List including 549 designations from January 1, 2024 through the end of the Biden administration on January 20, 2025. The vast majority of the entities added were from Russia and China with the UAE a distant third. Approximately 17% of entities on the Entity List were added in the last year, demonstrating an increasing emphasis on list-based enforcement.

There were fewer additions to the Unverified List ("UVL") during this same period—only 21 designations. BIS added eight persons to the UVL on October 16, 2024, from following destinations: China (3), Germany (2), Turkiye (2), and Pakistan (1). BIS added an additional 13 persons to the UVL on July 3, 2024, from following destinations: China (8), Cyprus (1), Kyrgyzstan (1), Turkiye (2), and the UAE (1).

C. BIS Antiboycott Enforcement Actions

In 2024, the U.S. continued its increasing enforcement of anti-boycott regulations, primarily governed by the EAR and the Ribicoff Amendment to the Tax Reform Act of 1976. These regulations are designed to prevent U.S. companies from participating in foreign boycotts that the United States does not sanction, such as the Arab League boycott of Israel. In 2024, BIS imposed a total of nearly $400,000 in antiboycott penalties on four companies:

- A civil penalty of $153,175 was imposed on January 29, 2024, against Wabtec Corporation ("Wabtec"), a global manufacturer and supplier of rail technology headquartered in Pennsylvania, to resolve 43 antiboycott violations that occurred when Wabtec failed to report Pakistan-origin boycott-related requests. Wabtec voluntarily disclosed the conduct to BIS, cooperated with the investigation by BIS's Office of Antiboycott Compliance ("OAC"), and implemented corrective actions after discovering the conduct at issue, which resulted in a significant penalty reduction.

- On June 3, 2024, BIS fined Airbus DS Government Solutions Inc. ("Airbus") $44,750 to resolve three antiboycott violations. Airbus participated in a trade show in Kuwait in 2019. In connection with the shipment of products and items for display at the trade show, the company furnished to its freight forwarder a commercial invoice/packing list certifying that the goods were not of Israeli origin and not manufactured by a company on the "Israeli Boycott Blacklist" in violation of Section 760.2(d) of the EAR. The company also failed to report to BIS, pursuant to Section 760.5 of the EAR, the receipt of the request to furnish this information. Airbus voluntarily disclosed the conduct to BIS, cooperated with the OAC's investigation, and implemented remedial measures leading to a significant reduction in the penalty.

- Similarly, on August 26, 2024, BIS imposed a civil penalty of $44,750 against Streamlight, Inc. ("Streamlight"), a global manufacturer of portable lighting products, resolving three antiboycott violations. Streamlight voluntarily self-disclosed the violations, cooperated with OAC's investigation, and implemented remedial measures earning a significant reduction in penalty. Similar to Airbus, the violations resulted from Streamlight's participation in a trade show in Bahrain in 2019. In connection with the export goods for display at the trade show, Streamlight furnished to its freight forwarder/logistics provider a commercial invoice/packing list certifying that the goods were not of Israeli origin and not manufactured by a company on the "Israeli Boycott Blacklist". The company also failed to report the request to BIS.

- On September 24, 2024, BIS imposed a civil penalty of $151,875 against Quantum Corporation, a data storage, management, and protection company, to resolve 45 alleged antiboycott violations relating to the failure to report the receipt of boycott requests from its customer, a distributor located in the United Arab Emirates ("UAE").

> Quantum Corporation submitted a voluntary disclosure, cooperated with OAC, and implemented remedial measures after discovering the conduct at issue, which resulted in a significant reduction in penalty. Assistant Secretary for Export Enforcement Matthew S. Axelrod emphasized that "[a] company with foreign subsidiaries, distributor agreements, or other contractual relationships in boycotting countries has extra work to do to amplify awareness of the antiboycott regulations among their foreign partners."

OAC also created the Boycott Requester List in March 2024, which is a public database of entities that have made a boycott-related request as reported to BIS. This list is intended to assist U.S. persons with complying with U.S. antiboycott laws as part of their screening and due diligence processes. Inclusion on the Boycott Requester List does not prohibit U.S. persons from dealing with entities on the list but, rather, serves as a red flag that the U.S. person should address during its due diligence efforts. OAC created a process by which listed entities can petition for removal by certifying to OAC that they will remove all boycott-related requests in documents and communications used with U.S. persons (including foreign subsidiaries). Indeed, more than 40 companies were removed from the Boycott Requester List in 2024 demonstrating some success in OAC's stick and carrot approach.

D. DDTC Enforcement Actions

In the past year, DDTC has been active, imposing civil penalties for violations of the Arms Export Control Act ("AECA") and the ITAR in connection with unauthorized exports and retransfers of technical data. DDTC entered into three consent agreements in 2024.

In February 2024, The Boeing Company ("Boeing") settled with DDTC in connection with unauthorized exports to China and violations of DDTC license terms and conditions. According to Boeing's voluntary disclosure, from 2013-2017 three employees in China, which is a proscribed destination under 22 C.F.R. 126.1(d)(1), downloaded ITAR-controlled technical data. Between 2013 and 2018, an indeterminate number of foreign-person employees and contractors working at Boeing and its partner facilities in 18 countries, including Australia, Canada, France, Germany, Hong Kong, India, Italy, Japan, Kenya, Morocco, Russia, Singapore, South Korea, Spain, Thailand, Taiwan, Ukraine, and the United Kingdom downloaded ITAR-controlled technical data. In addition, Boeing disclosed multiple additional unauthorized exports, reexports, retransfers, and temporary imports of defense articles, including technical data. In one instance, a trade compliance specialist working at Boeing's U.S. subsidiary, Aviall Services, Inc., fabricated five permanent export licenses, which resulted in the exporting of USML Category XIX(f)(1)-(3) nozzle segments and seal strips to Portugal and Turkey without DDTC authorization on seven occasions between July and November 2018. In other instances, Boeing involved itself in unauthorized exports due to several misclassifications and improperly relying on Department of Commerce authorizations. Lastly, Boeing failed to comply with several provisos of DDTC authorizations,

including illegal exports of technical data related to enhancements of, or upgrades to, integrated systems to the Government of Israel and two Israeli contractors, and the disclosure of U.S. Government data link capabilities to five pilots in the Lebanese Armed Forces.

As a result, DDTC imposed a $51 million penalty (with $24 million suspended on the condition that this amount will be used towards remedial compliance measures outlined in the Consent Agreement). Boeing agreed to two independent audits in addition to strengthening its compliance policies, procedures, and training, which will be implemented under the supervision of an external Special Compliance Officer for the entire three-year term of the Consent Agreement. DDTC credited extensive cooperation, and Boeing's agreement to take significant steps to improve its compliance program, as the reason DDTC did not issue a debarment. The consent agreement highlights the need to review compliance measures are adequately monitored and ensuring that proper authorizations are in place for the export of sensitive technical data, particularly when foreign-person employees will have access to such technical data. Additionally, it is crucial to have a well-trained and adequately resourced compliance team to properly review export control classifications in order to avoid misclassifications and faulty interpretations of DDTC authorizations.

In August 2024, RTX Corporation ("RTX") entered into a consent agreement with DDTC in connection with unauthorized exports, reexports and retransfers of defense articles to multiple countries, including proscribed destinations listed in 22 C.F.R 126.1, and violations of license terms, conditions and provisos of DDTC authorizations. RTX was charged with a total of 750 violations at the time. Since 2020, RTX submitted 27 voluntary disclosures demonstrating systemic failures to establish proper jurisdiction and classification of defense articles within certain operating divisions, resulting in the export/reexport of defense articles to 32 different countries without authorization, including to China. The majority of these voluntary disclosures and violations arose out of systematic jurisdiction and classification errors made by RTX's predecessor companies including Rockwell Collins, Inc. and United Technologies Corporation.

Since 2019, RTX also submitted several disclosures describing unauthorized exports of defense articles (including classified defense articles) to proscribed destinations, including on several occasions during employee travel through hand carrying company-issued laptops to proscribed destinations that included Lebanon, Russia, and Iran. Additionally, RTX submitted 36 disclosures related to its violations of the terms of DDTC authorizations on numerous occasions.

RTX agreed to pay a $200 million penalty (with a potential $100 million suspended on the condition that it be applied to remedial compliance costs as outlined in the consent agreement). Compliance measures included in the agreement consist of the appointment of an external Special Compliance Officer, an independent audit, and strengthening

compliance policies, procedures, training, and an automated export compliance system. DDTC credited extensive cooperation, and RTX's agreement to take significant steps to improve its compliance program, as the reason DDTC did not issue a debarment. The consent agreement highlights the need to conduct proper due diligence into a predecessor's compliance program, ensuring that any systematic failures, including misclassifications, are identified and remedied as soon as possible.

In October 2024, Precision Castparts Corp. ("PCC") entered into a consent agreement with DDTC in connection with unauthorized exports of technical data controlled under the United States Munitions List ("USML") Category XIX, to certain foreign person employees. PCC submitted a full voluntary disclosure describing unauthorized exports of technical data to certain foreign-person employees at its wholly owned subsidiary. Although these employees had lawful U.S. employment authorization, they were not covered by export authorizations.

PCC was fined a total of $3 million (with $1 million suspended on the condition that this amount be applied to remedial compliance costs as outlined in the consent agreement). It was also required to appoint an internal Special Compliance Officer for the entire term of the consent agreement, in addition to conducting an independent audit during this period. Other compliance measures include strengthening compliance policies, procedures, training, and implementing an automated export compliance system. Once again, the PCC consent agreement highlights the need to ensure proper pre- and post-acquisition due diligence is conducted to identify and quickly remediate ITAR compliance issues.

E. Outlook for Export Controls Enforcement in 2025

It is clear that the Trump administration will use export controls to pressure geopolitical adversaries, in particular China. Project 2025 contained numerous policy proposals on export controls including denying licenses to countries that do not permit adequate end-use checks, such as China and Russia, requiring BIS to make public recommendations for new controls on a quarterly basis, and promoting an open process between industry and export control agencies regarding emerging technologies that may need to be controlled.

On January 20, 2025, President Trump issued a memorandum providing the framework for an "America First Trade Policy," which requires the Secretaries of State and Commerce to "review the United States export control system and advise on modifications in light of developments involving strategic adversaries or geopolitical rivals as well as all other relevant national security and global considerations." Specifically, the memorandum directs t hat the Secretary of State and the Secretary of Commerce "shall assess and make recommendations regarding how to maintain, obtain, and enhance our Nation's technological edge and how to identify and eliminate loopholes in existing export controls - especially those that enable the transfer of strategic goods, software, services, and

technology to countries to strategic rivals and their proxies. In addition, they shall assess and make recommendations regarding export control enforcement policies and practices, and enforcement mechanisms to incentivize compliance by foreign countries, including appropriate trade and national security measures."

From an enforcement perspective, we would expect prioritization of matters involving China and Iran with the potential to use a threatened or actual expansion of export controls on Russia as a bargaining chip in negotiations to end the war in Ukraine. We also expect an even greater use of the Entity List and Unverified List with a continued focus on Chinese companies. As perhaps the most pro-Israeli administration in recent history, we expect the Trump administration to vigorously enforce anti-boycott laws and target Iran and its regional allies with additional export control enforcement actions. At the same time, U.S. companies that allegedly violate export control laws may, at least in some situations not directly conflicting with other administration priorities, see a more friendly enforcement environment as Attorney General Bondi has disbanded the NSD's Corporate Enforcement Unit.

III. U.S. Sanctions Enforcement Updates

In a surprising development, given public statements from senior Biden administration officials that sanctions enforcement would increase, OFAC enforcement activity declined in 2024 as compared with 2023.

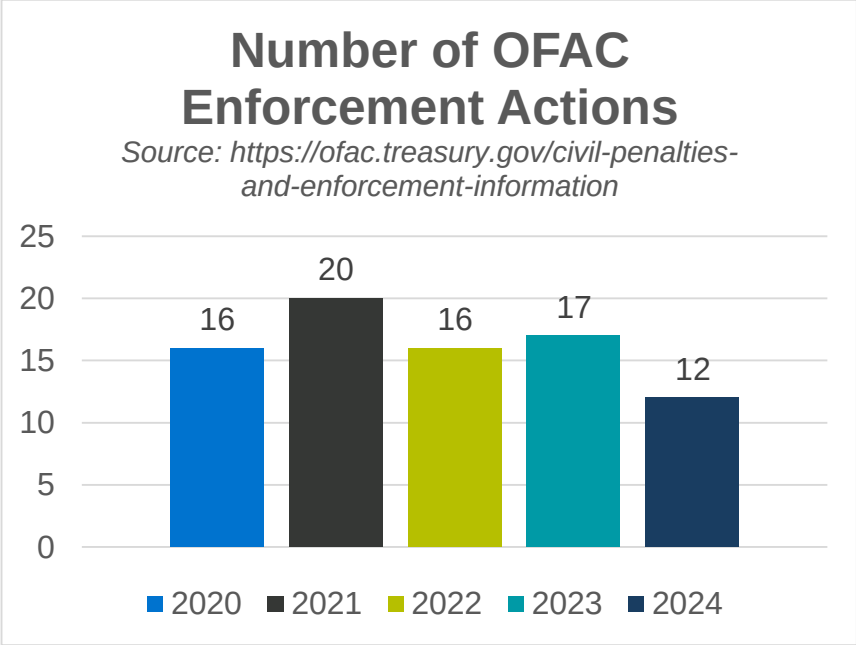
A. OFAC Enforcement Guidance and Announcements

On July 22, 2024, OFAC published guidance—summarized in our prior alert—regarding the statute of limitations extension, from 5 to 10 years, for violations of the International Emergency Economic Powers Act and the Trading with the Enemy Act. The statute of limitations for such violations was extended, on April 24, 2024, under the 21st Century Peace through Strength Act, Pub. L. No. 118-50. On September 11, 2024, as covered in a previous alert, OFAC issued an interim final rule, which comports with the above-described statute of limitations extension, that extended OFAC's recordkeeping requirements from 5 years to 10 years. This updated recordkeeping requirement went into effect on March 12, 2025.

Indicative of the Biden administration's efforts to coordinate with foreign governments to enforce U.S. sanctions, on October 9, 2024, OFAC entered a Memorandum of Understanding ("MOU") with the Office of Financial Sanctions Implementation ("OFSI") of the UK and Northern Ireland. In the MOU, containing mutual terms and conditions, the parties agreed to coordinate with each other to further their common goal "of investigating, enforcing, and promoting compliance with economic sanctions and certain trade sanctions promulgated by the" UK and U.S.—for example, by sharing relevant information and engaging in joint operations.

B. OFAC Enforcement Actions

OFAC was not as active in 2024. Throughout 2024, as shown in the chart below, OFAC announced only 12 enforcement actions in total and the largest reported settlement was for $20 million, with SCG Plastics. In comparison, in 2023, OFAC brought 17 enforcement actions, and the largest penalty was against Binance for over $968 million.



Nonetheless, the following OFAC enforcement actions bear mention as they tend to highlight some OFAC enforcement trends that may continue as 2025 unfolds.

- Transactions in or around Iran likely invite added scrutiny: 6 of the 12 OFAC enforcement actions from 2024 involved violations of Iranian sanctions. This, combined with the Trump administration's February 2025 announcement that it will restart its imposition of "maximum pressure on the Iranian regime," signals that transactions with Iranian parties are likely to be heavily scrutinized by OFAC.

- Foreign entities need to be vigilant to avoid "causing" U.S. persons to violate U.S. sanctions: 5 of the 12 OFAC actions in 2024 involved situations where a foreign person "caused" a U.S. person (e.g., a U.S. correspondent bank) to engage in sanctions violations. Given OFAC's longstanding warning that foreign entities will be held accountable in these scenarios, such entities need to ensure they focus on potential U.S. connections (even if not readily identifiable) that may result in OFAC violations, when completing a transaction—for example, clearing of USD payments through U.S. banks.

- Entities need to lookout for Russian persons' continued efforts to avoid U.S. sanctions: while, as noted above, the Trump administration may modify or curtail sanctions against Russia, two of the OFAC actions in 2024 were under the Ukraine-Russia sanctions program. Given the numerous Russia-related sanctions issued under the Biden administration that raised novel issues, some investigations may be ongoing and could result in enforcement actions in 2025. Indeed, in January 2025, OFAC settled with two different entities based on Russian sanctions violations.

C. Bank Majority-Owned by Turkish Government Not Immune from Criminal Prosecution for U.S. Sanctions Violations

As covered in a prior alert, on October 22, 2024, in *United States v. Turkiye Halk Bankasi A.S.*, the U.S. Court of Appeals for the Second Circuit ruled that Halkbank—a commercial bank, majority-owned by the government of Turkey—was not immune from criminal prosecution, for violations of U.S. sanctions against Iran. The Second Circuit considered common law immunity on remand from the U.S. Supreme Court, which found that Halkbank was not immune from criminal prosecution under the Foreign Sovereign Immunities Act ("FSIA"), because the FSIA only applies to civil—not criminal—cases. These decisions open the gates for some criminal prosecutions of foreign sovereigns and their instrumentalities, including for sanctions violations. The resulting potential impact of the decision is outlined in a previous publication.

D. U.S. Sanctions Enforcement Outlook for 2025

We expect that the Trump administration will continue the vigorous use of sanctions as a tool to achieve foreign policy objectives and will adjust U.S. sanctions to align with the administration's foreign policy. We would expect recalibration of the U.S. approach to Russia sanctions. The Biden administration, since the Russian invasion of Ukraine, has extended economic sanctions over many sectors of the Russian economy and has broadly used sanctions against Russian nationals who may be operating in sanctioned economic sectors and companies. More recently, the Biden administration had been focusing on imposing so-called secondary sanctions on persons alleged to be assisting Russia with evading sanctions, with a strong focus on Chinese entities. The incoming administration may seek to take a tougher line on Chinese evasion efforts while simultaneously signaling a willingness to offer Russia sanctions relief in exchange for a negotiated end to the conflict in Ukraine.

On the other hand, we anticipate that the incoming administration will increase its use of sanctions against Iran and Cuba, as well as Venezuela and Nicaragua. This would be in-line with the Trump administration's anticipated more hawkish approach to those countries. One area where we would expect a continuation of the current administration's approach is in the use of sanctions against companies tied to the Chinese military-industrial complex.

We note that OFAC has not instituted a country-specific sanctions program on China; rather it has used existing sanctions authorities to target specific Chinese persons and entities. In addition to the use of tariffs, the Trump administration could seek to increase pressure on China with a country-specific sanctions regime. Regardless of the adjustments in approach, we continue to expect robust sanctions enforcement and would caution businesses engaging in international trade, making international investments, or receiving in-bound foreign investment to continue to be diligent in their sanctions compliance efforts. Similarly, we would caution asset managers to conduct careful diligence on their international investments as well as incoming sources of investment to ensure compliance with the sanctions laws.

IV. DOJ Enforcement Updates

A. NSD's Enforcement Policy Update

On March 7, 2024, NSD issued an updated NSD Enforcement Policy for Business Organizations ("NSD Enforcement Policy"), which encourages voluntary self-disclosures to NSD and provides additional guidance on the criteria that NSD and other authorities use in determining an appropriate resolution in the voluntary self-disclosure context.

The most significant aspect of the updated Policy is the inclusion of an "M&A Policy" under which (and subject to certain exceptions) an acquiring company is entitled to "additional protections" for making a voluntary self-disclosure if it:

- completes a lawful, bona fide acquisition of another company;
- voluntarily and timely self-discloses to NSD potential criminal violations of laws affecting U.S. national security committed by the acquired entity;
- fully cooperates with NSD's investigation; and
- timely and appropriately remediates the misconduct.

Notably, the presence of aggravating factors at the acquiring company or the acquired company—such as a history of recidivism—does not automatically disqualify the acquiror from the additional protections. For qualifying companies, the M&A Policy describes the following benefits:

- NSD generally will not seek a guilty plea from the acquiror;
- The acquiror will not be required to pay a criminal fine or forfeit assets; and
- The misconduct disclosed to NSD will not affect NSD's assessment of the acquiror's history of recidivism in future matters involving the acquiror.

Not long after NSD put the policy into action, on May 22, 2024, two individuals pled guilty to wire fraud conspiracy for their role in a scheme to fraudulently procure products from a Massachusetts biochemical company, MilliporeSigma, and to export them to China using falsified export documents. Notably, when MilliporeSigma discovered that one of its employees was diverting biochemical products to an unauthorized purchaser in China, it retained outside counsel who, even before the conclusion of the company's internal investigation, promptly made a voluntary self-disclosure of the potential misconduct to NSD. This was rewarded with NSD's first-ever corporate declination of prosecution under its voluntary self-disclosure program. According to the DOJ, "MilliporeSigma offered exceptional cooperation . . . MilliporeSigma's cooperation allowed investigators to quickly identify the individuals responsible for the scheme . . . and secure their felony guilty pleas. As a result of MilliporeSigma's timely self-disclosure and extraordinary cooperation, MilliporeSigma will not be charged, despite the criminal wrongdoing committed by" one of its employees. This declination of prosecution demonstrates NSD's commitment to using its Enforcement Policy to encourage voluntary self-disclosures and cooperation from businesses, and its focus on individual accountability.

B. NSD Enforcement Actions

In 2024, NSD announced over 80 enforcement actions related to U.S. economic sanctions and export control laws, a significant increase from 2023 (68) and 2022 (31). Unsurprisingly, NSD's 2024 enforcement priorities focus on sanctions and export control violations involving foreign adversaries including Russia, Iran, and China.

These enforcement actions demonstrate a continued commitment to combatting sanctions evasion and money-laundering schemes. For instance, on April 19, 2024, two Florida-based steel traders were sentenced for their involvement in a scheme to violate U.S. sanctions on pro-Russian Ukrainian oligarch Sergey Kurchenko. Acting through an Orlando-based company, the traders illicitly traded with sanctioned individuals and entities and transferred over $150 million to Kurchenko and companies controlled by him in exchange for various metal products. As a result of their misconduct, one trader received a six-year prison sentence and was ordered to forfeit $160 million, and the other was sentenced to 21 months in prison and required to forfeit $4.7 million.

In another case, on February 2, 2024, seven individuals were charged for their involvement in a billion-dollar oil laundering network orchestrated by Iran's Islamic Revolutionary Guard Corps ("IRGC") and its Qods Force. The defendants—affiliates of the Qods Force, an Iranian shipping official, and Turkish nationals operating a Qods Force front company—allegedly partnered with entities located in Turkey, Lebanon, Russia, Oman, Greece, India, the UAE, Cyprus, and elsewhere to conceal the Iranian origin of the oil, and then launder the proceeds of the sales through layered transactions, bulk cash smuggling, and trade-based money laundering. This scheme allowed the Qods Forced to complete the delivery of millions of barrels of Iranian crude oil and petroleum products to buyers in Syria, Russia, and China. In furtherance of this scheme, billions of dollars were allegedly transferred through

the U.S. banking system, and the U.S. seized $108 million that IRGC front companies attempted to launder through U.S. financial institutions.

NSD enforcement actions in 2024 have also highlighted the extent of international cooperation in enforcing U.S. sanctions and export control laws. For example, on September 2, 2024, the DOJ announced the seizure of a Dassault Falcon 900EX aircraft, valued at approximately $13 million, which was allegedly used by Venezuelan President Nicolás Maduro and his associates. According to the DOJ, the aircraft was illicitly purchased through a shell company and smuggled from the United States for Maduro's use. In connection with the enforcement action, Attorney General Merrick B. Garland emphasized the "invaluable assistance by the authorities in the Dominican Republic[,]" where the seizure took place. In addition, the DOJ collaborated with authorities in Greece and Cyprus to secure the extraditions of two individuals accused of exporting U.S.-origin microelectronics to Russia in violation of U.S. export controls.

C. Disruptive Technology Strike Force

Launched in 2023 to prevent U.S. adversaries from illicitly acquiring sensitive technologies, the Disruptive Technology Strike Force ("DTSF") had an active year in 2024, in which it brought 15 criminal cases charging sanctions and export control violations, smuggling conspiracies, and other offenses related to the transfer of sensitive information, goods, and military-grade technology to China, Russia, and Iran.

On August 15, 2024, as a result of DTSF's interagency effort, BIS imposed a $5.8 million penalty on TE Connectivity and its Hong Kong subsidiary for exporting restricted items—such as printed circuit-board connectors and pressure and temperature scanners—to Chinese entities. TE Connectivity voluntarily disclosed these violations and cooperated with the investigation, which was taken into account in the penalty assessment. As BIS noted, this case underscores the importance of strict adherence to export control regulations, even for low-level technologies, and highlights the benefits of voluntary self-disclosure and cooperation with enforcement authorities.

To develop its presence in locations of critical technology-related industries, DTSF also opened new offices in Texas, Georgia, and North Carolina, expanding its geographical reach from 14 to 17 locations. Further, DTSF broadened its interagency collaboration by adding the Defense Criminal Investigative Service as a Strike Force law enforcement partner.

International collaboration was also on the rise. On April 26, 2024, the DOJ and Department of Commerce, together with South Korea and Japan, initiated the Disruptive Technology Protection Network. This network was created after an August 2023 summit between the heads of these countries, where they agreed to increased collaboration and information sharing with respect to technology protection measures, including establishing connections between DTSF representatives and their South Korean and Japanese counterparts.

In 2025, as technology-related national security concerns continue to grow, DTSF is likely to intensify its enforcement activities to protect disruptive technologies from foreign adversaries. While the scope of "disruptive technologies" is unclear, DTSF is expected to continue focusing on sensitive technologies including supercomputing and exascale computing, AI, advanced manufacturing equipment and materials, quantum computing, and biosciences. Notably, former Deputy Attorney General Lisa O. Monaco—who announced the creation of DTSF in 2023—has stated that DTSF "will place AI at the very top of its enforcement priority list. After all AI is the ultimate disruptive technology." The emphasis will likely be on China, the U.S.'s biggest competitor in the AI field. Indeed, Commerce Secretary Howard Lutnick, in his confirmation hearing, pointed to the recent Deepseek AI announcement as evidence of China's misuse of American technology and said that he is "thrilled to coordinate [with] and empower BIS" to stop China from using American tools to compete against the U.S.

D. Outlook for DOJ Enforcement in 2025

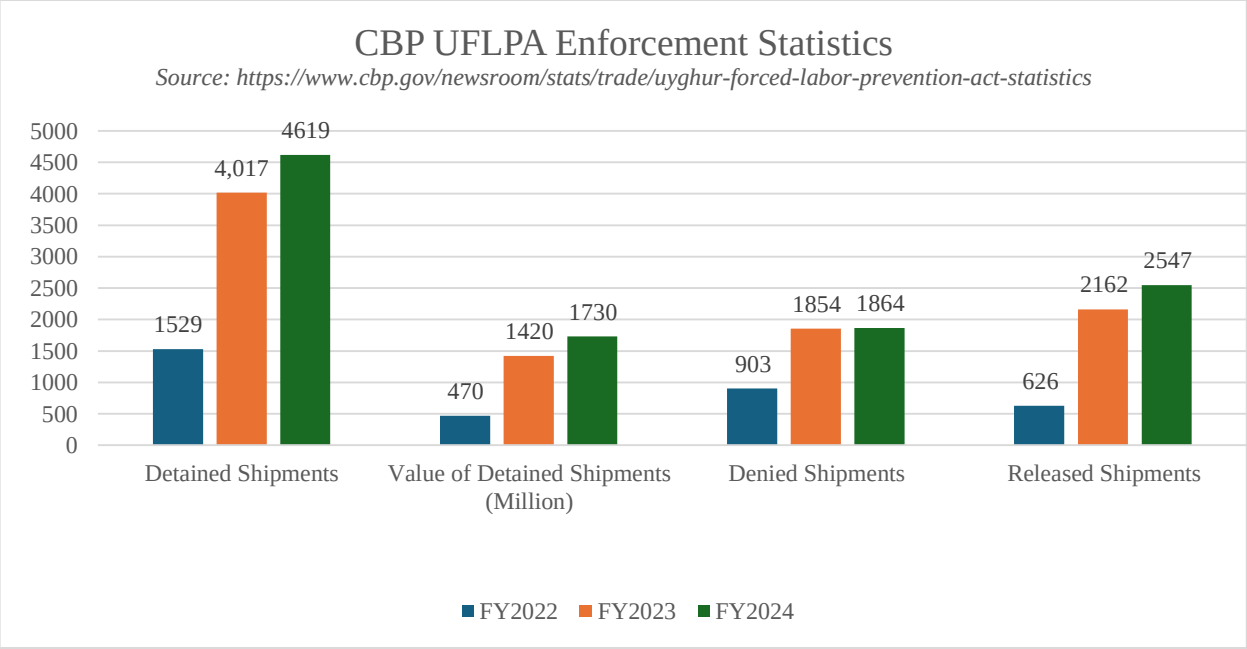
Early indications from the Trump administration appear to signal a reduction in the level and intensity of enforcement actions against U.S. companies who violate international trade laws. From disbanding the NSD's Corporate Enforcement Division to pausing enforcement of the Foreign Corrupt Practices Act, the focus appears to be shifting toward more heavily focusing on criminal conduct by individuals (with companies who assist in those investigations being rewarded for their cooperation), likely paired with targeted enforcement actions against individuals and entities connected to certain disfavored jurisdictions such as China and Iran. Vice President Vance has also indicated that the U.S. could significantly increase sanctions and enforcement activity related to Russia if it does not negotiate in good faith to end the war in Ukraine.

V. Forced Labor Enforcement Updates

A. Forced Labor Enforcement Actions

In 2024, the U.S. intensified its efforts to combat forced labor, particularly under the Uyghur Forced Labor Prevention Act ("UFLPA"). The UFLPA imposes a rebuttable presumption that goods produced, in whole or in part, in the Xinjiang Uyghur Autonomous Region ("XUAR") of China, or produced by entities on the UFLPA Entity List, are made with forced labor and thus prohibited from entering into the U.S.

In FY2024 (October 1, 2023 to September 30, 2024), U.S. Custom and Border Protection ("CBP") detained 4,619 shipments—with a combined value of $1.73 billion—under the UFLPA. Of these shipments, 1,864 were eventually denied entry. As the graph below shows, the statistics for FY2024 show an increase from prior years in terms of the number of detained shipments, the value of detailed shipments, and the number of denials.



Consistent with FY2023, the top three categories of shipments subject to UFLPA-related CBP detainment in FY2024 are electronics (2,623), apparel, footwear, and textiles (876), and industrial and manufacturing materials (310). In terms of country of origin, the vast majority of detained shipments originated from Southeast Asian countries including Vietnam ($0.55 billion), Malaysia ($0.49 billion), and Thailand ($0.44 billion). This demonstrates the global reach of UFLPA enforcement, as CBP recognizes that raw materials or components originating from XUAR may be comingled, transshipped, and/or otherwise altered to obscure their XUAR nexus. In 2024, the Department of Homeland Security's ("DHS") Forced Labor Enforcement Task Force, an interagency team with the mandate of preventing the importation of goods made with forced labor into the U.S., added 73 entities to the UFLPA Entity List—a significant increase from 19 in 2023 and 27 in 2022. The importation of goods produced by entities on the UFLPA Entity List is subject to a rebuttable presumption that the goods are made with forced labor and prohibited from entry to the United States.

Congress also demonstrated consistent support for UFLPA enforcement efforts. For example, congressional lawmakers issued letters to DHS in January, April, June, and October, advocating for significant expansions to the UFLPA Entity List across various industries such as apparel, batteries, critical minerals, and pharmaceuticals. Additionally, a bipartisan letter sent to the U.S. Trade Representative in September emphasized the need for greater collaboration between the U.S., Canada, and Mexico to prevent UFLPA circumvention.

In 2024, CBP and DHS issued three withhold release orders ("WROs") and one forced labor finding ("Finding"). WROs are issued when CBP has reasonable evidence of the use of forced labor in the manufacturing or production of goods entering the U.S., whereas CBP findings are issued by CBP upon determining that products intended for import into the U.S. are made, in whole or in part, with forced labor. WROs and Findings allow CBP, respectively, to

either detain the goods until the importer proves the absence of forced labor in the goods' supply chain or seize such goods.

On December 4, 2024, CBP issued a Finding against Kingtom Aluminio S.R.L. ("Kingtom"), a Chinese-owned aluminum extruder in the Dominican Republic. The Finding was based on the determination that Kingtom has used convict, forced, or indentured labor to produce aluminum extrusions, profile products, and derivatives, in violation of 19 U.S.C. § 1307, which prohibits the importation of any product "mined, produced, or manufactured wholly or in part in any foreign country by convict labor or/and forced labor or/and indentured labor." As a result of this Finding, Kingtom's goods are subject to immediate seizure at all ports of entry in the U.S.

On April 10, 2024, CBP issued a WRO against a Chinese company, Shanghai Select Safety Products Company, Limited, and its subsidiaries due to evidence of the use of convict labor in their production of work gloves. On November 1, 2024, CBP issued a WRO against Somaliland-based supplier Asli Maydi after finding reasonable evidence that the supplier used forced labor in its production of frankincense and frankincense-based products, which are often used in fragrance and skincare products.

On October 11, 2024, CBP modified the WRO against Brightway Group, a Malaysian glove manufacturer, noting that "[f]acilitation of legitimate trade is just as important as CBP's enforcement against illegal trade practices. When companies can document compliance with U.S. trade laws, forced labor or otherwise, they'll have access to the U.S. market." The WRO was initially imposed on Brightway on December 20, 2021. Following an extensive review, CBP found that "[s]ince the implementation of the WRO, the Brightway Group has taken actions to fully remediate the forced labor indicators within its manufacturing process."

B. Outlook for 2025

In 2025, we anticipate the Trump administration will continue enhancing forced labor-related enforcement actions particularly in connection with geopolitical rivals and in tandem with trade-related disputes. Recently, CBP has indicated that that its fight against forced labor "is far from over" and called for "continuous, collective effort—from governments, industries, and consumers—to ensure a world where no one's humanity is traded for profit." Marco Rubio, co-author of the Uyghur Forced Labor Prevention Act ("UFLPA") and active supporter for addressing human rights issues in XUAR, will certainly push the administration to pursue vigorous enforcement policies on forced labor issues, particularly in regards to China.

VI. CFIUS Enforcement Updates

A. CFIUS Enforcement Actions

As covered in a previous client alert, on July 23, 2024, the Committee on Foreign Investment in the United States ("CFIUS") published its Annual Report to Congress for the Calendar Year 2023 ("2023 Annual Report"). The report provides key statistics on the CFIUS process and

the transactions that were filed in 2023. Even though 2023 was a busy year for CFIUS, the number of declarations and notices filed decreased compared to previous years. Nevertheless, CFIUS demonstrated its commitment to increasing enforcement by imposing penalties for violations of mitigation agreements. In instances of non-compliance with mitigation agreements, CFIUS usually imposes measures to address the non-compliance, and in the event of a material breach, it might impose monetary penalties. In 2023, CFIUS imposed a record of four civil penalties for material breaches and the first under the regulations implementing the Foreign Investment Risk Review Modernization Act; prior to this, CFIUS had only assessed two civil monetary penalties in its nearly 50-year history.

Soon after publishing the 2023 Annual Report, in August 2024, CFIUS provided an update on its enforcement actions taken in 2023 and 2024. As of August 2024, CFIUS had imposed three penalties in 2024, including:

- a $60 million penalty against T-Mobile US, Inc. ("T-Mobile") for violating a National Security Agreement ("NSA"), entered into in 2018 in connection with its merger with Sprint, by failing to take appropriate measures to prevent unauthorized access to certain sensitive data and failing to report some incidents of unauthorized access promptly to CFIUS.

- a $1.25 million penalty, the maximum allowed under CFIUS' regulations, against a foreign acquirer for submitting a joint voluntary notice and supplemental information containing five material misstatements, including forged documents and signatures. CFIUS rejected the filing as a result of the misstatements, and the transaction was abandoned.

- Following an initial Notice of Penalty issued earlier in the year, CFIUS resolved an enforcement action against a party to an NSA, resulting in an $8.5 million penalty. CFIUS determined that the company's majority shareholders orchestrated an initiative to remove all of the company's independent directors, thereby causing the Security Director position to be vacant and the board of directors' government security committee to be defunct, resulting in a breach of the NSA.

These penalties are notable for several reasons including that the $60 million T-Mobile penalty was the largest ever imposed by CFIUS, and the penalty related to material misstatements made in connection with CFIUS filings was the first ever imposed for such a violation.

In November 2024, Treasury published a final rule that, among other changes, increased the maximum civil penalty for violations of statutory or regulatory provisions (or agreements, conditions, or orders issued pursuant thereto) as follows:

Nature of Violation	Previous Maximum Civil Monetary Penalty Per Violation	Maximum Civil Monetary Penalty Per Violation
Submitting a declaration, notice, or response to request for information with a material misstatement or omission or making a false certification	$250,000	$5,000,000
Failure to file a mandatory declaration	The greater of $250,000 or the value of the transaction	The greater of $5 million or the value of the transaction
Violating, intentionally or through gross negligence, a material provision of a mitigation agreement	The greater of $250,000 or the value of the transaction	The greater of $5 million or the value of the transaction

It is clear that CFIUS is prioritizing enforcement in order to ensure compliance with regulatory and other legal requirements.

Although not an enforcement action by CFIUS itself, the Biden administration's decision on January 3, 2025, to block Japanese company, Nippon Steel, from acquiring U.S. Steel, has led CFIUS practitioners and observers to question whether the CFIUS review process will become increasingly politicized.

B. Outlook for CFIUS Enforcement in 2025

We would expect the Trump administration to continue the Biden administration's focus on inbound investment from China and other adversaries and possibly even expand the scope of national security review of inbound investments by CFIUS. The Biden administration increased its scrutiny of Chinese investment into critical and emerging technology companies, particularly in the biotech and AI spaces. Under the Trump administration, we would expect that in-bound Chinese investment into more traditional areas of the economy, such as manufacturing, would also receive heightened scrutiny. CFIUS could also become a protectionist tool used to review in-bound investment by foreign nationals from U.S. allies, such as Japan, that could result in a change of control of U.S. manufacturing and energy businesses to foreign ownership. Project 2025 calls for CFIUS to be strengthened including by developing a more robust mitigation monitoring program, expanding its jurisdiction to greenfield investments, and imposing more penalties for regulatory violations.

As illustrated by the increase in number of enforcement actions reported to Congress, CFIUS will likely increase enforcement activity, especially in regard to parties that fail to submit mandatory filings or violate mitigation agreements. We expect CFIUS will continue to carefully scrutinize both notified and non-notified transactions involving key industries, including life sciences, semiconductors and advanced computing, cybersecurity, and aerospace, among others. There may, however, be less sensitivity around foreign investments in clean energy given the Trump administration's deemphasis of climate-related technologies as compared to the Biden administration.

VII. EU Sanctions Enforcement

Since the beginning of Russia's invasion of Ukraine, the EU has gradually increased the breadth and depth of sanctions against Russia and Belarus through the adoption of 15 sanction packages imposing both individual and sectoral restrictions to hinder Russia's ability to wage war. In the meantime, enforcement activities have continued to ramp up in various countries notably focusing recently on anti-circumvention, despite the lack of a common enforcement framework in the EU. In this context, 2024 has brought significant updates to the EU sanctions regulatory framework, particularly in addressing circumvention. This has notably let to the introduction of a "best-efforts" obligation, a broader definition of the notion of circumvention, and a due diligence obligation related to the re-export of certain sensitive items to Russia through third countries. More details on these regulations will be published in our upcoming review of EU regulatory developments.

A. New EU Directive on the Definition of Criminal Offenses and Penalties for Sanctions Violations

1. Background and Objectives

On July 3, 2024, the European Parliament issued a briefing highlighting concerns regarding the implementation and enforcement of EU sanctions by Member States.

The decentralized approach to enforcement has resulted in inconsistencies, including:

- a lack of criminal prosecutions for sanctions violations;
- variability in penalty levels among Member States (ranging from €133,000 to €37.5 million);
- disparate treatment of sanctions violations:
  - 12 Member States treat sanctions violations as a criminal offense;
  - 13 Member States categorize it as a criminal or an administrative offense;
  - 2 Member States consider it only an administrative offense;

- in countries where sanctions violations are classified as criminal offenses, punishments may include imprisonment that can vary significantly, from a maximum of 2 years to a maximum of 12 years.

To address these concerns, the European Commission first proposed harmonizing the enforcement of EU sanctions by including sanctions violations in the list of EU crimes under article 83(1) TFEU (a necessary step for allowing EU action in this area). This allowed, on April 24, 2024, the adoption of Directive (EU) No 2024/1226 of the European Parliament and of the Council of 24 April 2024 on the definition of criminal offences and penalties for the violation of Union restrictive measures and amending Directive (EU) No 2018/1673, establishing minimum standards for criminal offenses and penalties for violations of EU restrictive measures (the "Directive").

The Directive entered into force on May 19, 2024, and must be implemented by Member States by May 20, 2025. Until Member States implement the Directive, we expect enforcement to continue in a decentralized manner, following the enforcement priorities set by each Member State.

2. Key Provisions

The Directive introduced several key provisions regarding:

- common minimum rules concerning the scope of criminal conduct violating EU restrictive measures: the Directive requires EU Member States to ensure that a comprehensive list of conduct related to sanctions violations constitutes a criminal offense when intentionally committed (e.g. failing to freeze assets belonging to designated persons or entities, breaching travel bans and arms embargoes). The Directive's article 3 (3.) also requires Member States to ensure that the provision of services related to prohibited items constitutes a criminal offence if committed with serious negligence, at least where that conduct relates to items included in the Common Military List of the European Union or to dual-use items listed in Annex I and IV to Regulation (EU) 2021/821;

- penalties: sets basic standards for penalties across all EU Member States that must be effective, proportionate, and dissuasive. Notably, article 8 of Regulation 833/2014 already upholds a similar standard. Serious violations should carry a minimum of five years' imprisonment in addition to financial penalties. For companies, the minimum penalty is the greater of 5% of global turnover or €40 million;

- investigation and prosecution: establishes minimum investigation and prosecution periods, fosters cooperation among Member States, and mandates proactive internal investigation by companies into potential sanctions violations;

- mitigating circumstances: introduces incentives for compliance, such as reduced penalties for voluntary self-disclosures, when providing the national competent authority information it would not have been able to otherwise obtain. Notably, Recital 26 of the Council Regulation (EU) 2024/1745 of 24 June 2024 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilizing the situation in Ukraine resulting from the 14th package, explicitly references this provision and its implementation by Member States.

In this ever-evolving context, it will be interesting to monitor how the Directive's provisions will be transposed into each Member States' national legal framework.

As an example, in France, despite the current legal framework, in particular article 459 of the Customs Code, French law will have to (i) introduce new specific offenses, such as intentional circumvention of sanctions, and (ii) strengthen the criminal liability of legal persons.

Moreover, in its 2024 annual report, the PNF (the French prosecuting authority for economic crimes), expressly referred to the Directive to extend its jurisdiction to economic sanctions violations/circumvention. This development could potentially significantly increase the enforcement of sanctions violations/circumvention in France.

B. EU Enforcement Framework

First and foremost, it is important to highlight that many enforcement measures undertaken by public authorities to punish breaches of EU sanctions are not systematically made public. For instance, in France, the mechanism of "composition pénale"—an alternative to prosecution—allows the offender to be held accountable while avoiding a formal trial. Once the measure is executed, public prosecution is extinguished, meaning the public prosecutor can no longer initiate proceedings against the offender. Moreover, not all competent national authorities officially disclose their enforcement statistics. The combination of these two factors significantly limits the availability of comprehensive data on enforcement actions. Below are examples of enforcement actions taken by national competent authorities in EU Member States regarding economic sanctions breaches or circumvention.

1. The Netherlands

- October 4, 2024: the District Court of Rotterdam convicted the director of an aeronautics company for violating EU sanctions by exporting aircraft parts to Russian airlines. The court sentenced the director to 32 months in jail, as well to the confiscation of €7,416.33 and €250,000 in cash, and, finally, the forfeiture of all his stock-in-trade and business accounts; the company itself was fined €165,826.

- September 23, 2024: the Dutch Public Prosecution Service (hereafter "PPS") reached an out of court settlement with an Amsterdam-based company for (i) violating EU sanctions by paying out dividends of approximately €18 million to one of its shareholders, a Russian company that is designated under the EU's Russian sanctions list since 2018 and (ii) circumventing EU sanctions by not having frozen the shares and suspended the associated voting rights. The director was fined €20,000 and the company €195,000.

- November 28, 2024: the District Court of Amsterdam fined a Dutch company, a developer and manufacturer of foundation equipment, €120,000, following the procedural agreements negotiated with the PPS, for violating EU and Dutch sanctions—imposed in response to Russia's occupation of Crimea—for selling goods and providing services for the construction of the bridge between Crimea and mainland Russia.

2. Latvia

- October 28, 2024: the State Revenue Service of Latvia initiated 94 criminal proceedings in 2024 for EU Russia and Belarus economic sanctions violations. Additionally, over 2,400 instances of blocked imports and exports were reported in 2024.

- December 6, 2024: The Kurzeme District Court sentenced the former editor-in-chief of Sputnik Latvia to two years in prison for violating EU sanctions. He continued to provide services to the Russian state propaganda agency Rossiya Segodnya, whose owner, Dmitry Kiselyov, has been on the EU sanctions list since March 21, 2014, because of his role as a central figure of the government propaganda campaign supporting the deployment of Russian forces in Ukraine.

3. Estonia

- June 2024 onwards: Estonia conducted over 240 inspections of vessels suspected of transporting sanctioned Russian oil, focusing on Russia's 'Shadow Fleet'. The inspections included "radio calls," physical checks, and document verifications. Inspections were based on the EU economic sanctions measures regarding circumvention of sanctions by Russian tankers. These vessels are under close surveillance as they could, potentially, transport oil bought above the G7 imposed price-cap. According to the head of the maritime department at the Ministry of Climate, most ship captains cooperated with authorities and provided compliant documentation.

- The Estonian Internal Security Service, under the Prosecutor's Office, is currently investigating and has taken into custody an individual on suspicion of managing funds for a sanctioned foundation.

C. What to Expect in 2025

Despite the renewal of existing sectoral sections and the adoption of the 16th sanctions package in February 2025, the existing policy disagreements regarding Russia between EU countries will likely also be witnessed in the way economic sanctions violations are enforced in the EU. As an example, countries like Poland or Spain who strongly support Ukraine are likely to intensify enforcement of sanctions violations whereas countries having divergent interests such are Hungary or Slovakia might be reluctant to do so.

VIII. UK Economic Sanctions Update

A. Creation of New Trade Sanctions Authority: The Office of Trade Sanctions Implementation

On September 12, 2024, the UK adopted a new regulation, "The Trade, Aircraft and Shipping Sanctions (Civil Enforcement) Regulations 2024", which came into force on October 10, 2024. One of the principal outcomes of this regulation is the establishment of a new regulatory authority within the Department of Business and Trade, namely the Office of Trade Sanctions Implementation (hereafter "OTSI").

OTSI's responsibilities can be categorized below:

- preventive measures: OTSI supports businesses in achieving compliance by clarifying the sanction regimes, enhancing understanding, and assisting entities in fulfilling their obligations;

- enforcement measures:

    - OTSI is responsible for the civil enforcement of trade sanctions that pertain to UK services and international trade involving goods and services that do not physically enter the UK territory. The OTSI has the authority to:

        - impose financial penalties and publicly disclose instances of non-compliance;

        - request information from relevant entities;

        - enforce sector-specific reporting obligations;

- OTSI and the OFSI both play key roles in enforcing economic sanctions, but they focus on different areas:

    - OFSI is part of His Majesty's Treasury and is responsible for financial sanctions enforcement including asset freezes, restrictions on financial services, and ensuring compliance by financial institutions. It issues financial penalties for the breach of financial sanctions;

    - OTSI is part of the Department for Business and Trade and is responsible for trade sanctions enforcement such as restrictions on exports, imports, and the provision of services to sanctioned entities. It works on compliance and enforcement for businesses engaged in international trade;

- OTSI works in coordination with His Majesty's Revenue and Customs ("HMRC") - whose role includes overseeing the import and export of goods, the transfer of technology to and from the UK, and ancillary services such as brokering and financial services related to trade activities - which is responsible for criminal enforcement of trade sanctions.

B. Mandatory Reporting Obligations, Fines for Unlicensed Exports and Key Enforcement Actions

On November 14, 2024, the UK amended its sanctions regime through the Sanctions (EU Exit) (Miscellaneous Amendments) (No. 2) Regulations 2024, which introduced a new reporting requirement for designated persons. Under this requirement, sanctioned individuals must disclose their global and UK-based assets to His Majesty's Treasury, as applicable, and report any changes to these assets. On December 5, 2024, the OTSI updated its guidance on sanctions against Russia to clarify that individuals subject to sanctions must report any changes in assets exceeding £10,000.

Notable enforcement actions taken by UK authorities include the following:

- January 22, 2024: the National Crime Agency arrested Dmitry Ovsyannikov, former mayor of Sevastopol, on charges of sanctions violations and money laundering. The charges involve opening a bank account at Lloyds Banking Group and depositing £76,000. This represents the first sanctions-related arrest under the UK's post-Brexit sanctions regime. Ovsyannikov pleaded not guilty on January 23rd 2024 with a trial scheduled for March 2025;

- between January and March 2024: HMRC issued settlement offers totaling over £2.3 million to seven UK exporters for violations under The Export Control Order 2008 and Retained Regulation 428/2009. These settlements addressed unlicensed exports of

military and dual-use goods. Key settlements included: £971,726 in February for unlicensed military exports; and £1,058,781 in March for unlicensed dual-use goods exports;

- August 29, 2024: the Office of Financial Sanctions Implementation imposed a £15,000 penalty on a UK-based concierge company for failing to comply with reporting obligations under the Gas and Electricity General License.

These enforcement actions showcase the UK's active approach to sanctions enforcement, notably relating to Russia. Given the current geopolitical context, and the closer ties between the EU and UK, we are expecting a stronger collaboration to enforce sanctions violations, which could lead to further enforcement actions in the UK.

C. UK Sanctions Enforcement Outlook for 2025

In 2025, the UK is expected to continue its close cooperation with the EU on policies, implementation, and enforcement of economic sanctions, particularly those targeting Russia. This alignment is notably evidenced in the joint response to the Russian 'Shadow Fleet'; as detailed in the call to action, issued on July 19, 2024, and last updated on November 28, 2024, with endorsement from third countries.

Additionally, on January 13, 2025, the OFSI and OFAC signed a Memorandum of Understanding **("MoU")**. This agreement aims at enhancing information sharing between the two agencies, facilitating the exchange of data relevant to the implementation and enforcement of economic sanctions. While the MoU underscores the robust collaboration between these authorities, its future under the Trump administration remains uncertain.

Authors

Luciano Racco
Co-Chair, International Trade & National Security – *Washington, DC*
+1.202.261.7319
lracco@foleyhoag.com

Anthony Mirenda
Partner – *Boston*
+1.617.832.1220
amirenda@foleyhoag.com

Olivier Dorgans
Partner - *Paris*
+33.(0)1.70.87.43.70
odorgans@foleyhoag.com

Paul Charlot
Counsel – *Paris*
+33.(0)1.70.87.43.71
pcharlot@foleyhoag.com

Nicholas Alejandro Bergara
Associate – *New York*
+1.212.812.0415
nbergara@foleyhoag.com

Aleksis Fernandez Caballero
Associate – *Boston*
+1.617.832.1239
afernandezcaballero@foleyhoag.com

Chawkat Ghazal
Associate – *Boston*
+1.617.832.1198
cghazal@foleyhoag.com

Camille Mayet
Associate – *Paris*
+33.(0)1.70.87.43.72
cmayet@foleyhoag.com

Zihan Mei
Associate – *Boston*
+1.617.832.1711
zmei@foleyhoag.com

Pauline Montaldier
Associate – *Paris*
+33.(0)1.70.87.43.74
pmontaldier@foleyhoag.com