Department of Commerce, Department of the Treasury, and Department of Justice Tri-Seal Compliance Note:

Obligations of foreign-based persons to comply with U.S. sanctions and export control laws

OVERVIEW

Today's increasingly interconnected global marketplace offers unprecedented opportunities for companies around the world to trade with the United States and one another, contributing to economic growth. At the same time, malign regimes and other bad actors may attempt to misuse the commercial and financial channels that facilitate foreign trade to acquire goods, technology, and services that risk undermining U.S. national security and foreign policy and that challenge global peace and prosperity. In response to such risks, the United States has put in place robust sanctions and export controls to restrict the ability of sanctioned actors to misuse the U.S. financial and commercial system in advance of malign activities.

These measures can create legal exposure not only for U.S. persons, but also for non-U.S. companies who continue to engage with sanctioned jurisdictions or persons in violation of applicable laws. To mitigate the risks of non-compliance, companies outside of the United States should be aware of how their activities may implicate U.S. sanctions and export control laws. This Note highlights the applicability of U.S. sanctions and export control laws to persons and entities located abroad, as well as the enforcement mechanisms that are available for the U.S. government to hold non-U.S. persons accountable for violations of such laws, including criminal prosecution. It further provides an overview of compliance considerations for non-U.S. companies and compliance measures to help mitigate their risk.

APPLICABILITY OF U.S. SANCTIONS AND EXPORT CONTROL LAWS TO FOREIGN-BASED PERSONS

U.S. Sanctions Laws

In furtherance of the national security and foreign policy interests of the United States, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) administers and enforces economic and trade sanctions, primarily against targeted foreign jurisdictions and

Date: March 6, 2024

regimes, as well as individuals and entities such as terrorists, international narcotics traffickers, weapons of mass destruction proliferators, and other malign actors.

OFAC sanctions take various forms, including blocking the property of specific individuals and entities, restricting a narrower range of dealings with specified actors, and prohibiting transactions involving an entire jurisdiction or country, such as through a trade embargo or sanctions related to particular economic sectors. "Blocking" refers to freezing assets or other property subject to U.S. jurisdiction and immediately imposes an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

OFAC may impose sanctions on persons engaging in specified conduct, as well as those engaging in deceptive transactions or dealings to circumvent OFAC sanctions programs, or on persons that materially assist, sponsor, or provide financial, material, or technological support for, or goods or services to or in support of, sanctioned persons or sanctionable activities.

OFAC's authority to impose sanctions is distinct from its enforcement authorities. U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons within the United States, and all U.S.-incorporated entities and their foreign branches. In certain sanctions programs, foreign entities owned or controlled by U.S. persons also must comply with applicable restrictions.[1] Certain sanctions programs also require foreign persons in possession of U.S.-origin goods to comply.

Non-U.S. persons are also subject to certain OFAC prohibitions. For example, non-U.S. persons are prohibited from causing or conspiring to cause U.S. persons to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions.

Violations of OFAC regulations may result in civil or criminal penalties.[2] OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a person subject to U.S. jurisdiction may be held civilly liable even if such person did not know or have reason to know that it was engaging in a transaction that was prohibited under sanctions laws and regulations administered by OFAC. OFAC's Economic Sanctions Enforcement Guidelines provide more

[1] *See e.g.*, 31 C.F.R. §560.215 (prohibiting foreign persons owned or controlled by a U.S. person from engaging in any transaction with the Government of Iran or subject to Iranian jurisdiction); 31 C.F.R. §515.329 (extending Cuba sanctions prohibitions to any corporation, partnership, association, or other organization, wherever organized or doing business, that is owned or controlled by U.S. persons); 31 C.F.R. §510.214 (extending certain North Korea sanctions to foreign persons owned or controlled by a U.S. financial institution).

[2] Civil penalties vary by sanctions program, and the Federal Civil Penalties Inflation Adjustment Act of 1990, as amended by the Federal Civil Penalty Inflation Adjustment Act Improvements Act of 2015, requires OFAC to adjust civil monetary penalty amounts annually. Current penalty amounts are available in OFAC's Economic Sanctions Enforcement Guidelines. *See* 31 C.F.R. Part 501, App'x A. For example, violations of IEEPA result in up to $386, 136 for violation. A list of select OFAC enforcement actions, organized by year, are available on the Civil Penalties and Enforcement Information page on OFAC's website. *See* Office of Foreign Assets Control, "Civil Penalties and Enforcement Information," *available at* https://ofac.treasury.gov/civil-penalties-and-enforcement-information.

information regarding OFAC's enforcement of U.S. economic sanctions, including the factors that OFAC generally considers when determining an appropriate response to an apparent violation.[3]

OFAC Enforcement Actions Against Foreign Persons

OFAC has actively employed its enforcement authorities against foreign financial institutions and other foreign persons who have, among other things, caused U.S. persons to violate OFAC sanctions, conspired to do so, indirectly exported services from the United States, or otherwise engaged in violative conduct. Examples of this conduct include when a non-U.S. person:

- Obscures or omits reference to the involvement of a sanctioned party or jurisdiction to a financial transaction involving a U.S. person in transaction documentation;
- Misleads a U.S. person into exporting goods ultimately destined for a sanctioned jurisdiction;[4] or
- Routes a prohibited transaction through the United States or the U.S. financial system, thereby causing a U.S. financial institution to process the payment in violation of OFAC sanctions.

Recent OFAC enforcement actions targeting such conduct include the following:

- In April 2022, Toll Holdings Limited ("Toll"), an international freight forwarding and logistics company headquartered in Australia, agreed to pay $6,131,855 to settle its potential civil liability for 2,958 apparent violations of multiple OFAC sanctions programs. Toll's liability arose when it originated or received payments through the U.S. financial system in connection with shipments made by Toll or its affiliates or suppliers involving the Democratic People's Republic of Korea, Iran, and Syria—all jurisdictions broadly subject to OFAC sanctions. Toll additionally conducted transactions involving the property or interests in property of blocked entities. In doing so, Toll caused U.S. financial institutions to transact with blocked persons and export financial services to sanctioned jurisdictions. OFAC determined that Toll acted recklessly by failing to adopt or implement policies that prevented it from conducting potentially violative transactions.[5]

- In July 2021, Alfa Laval Middle East Ltd. ("AL Middle East"), a UAE-based subsidiary of a foreign parent, settled with OFAC for $415,695 arising from two apparent violations. The

[3] 31 C.F.R. part 501, App'x A

[4] Department of Commerce, Department of the Treasury, Department of Justice, Department of State, and Department of Homeland Security Quint-Seal Compliance Note: Know Your Cargo: Reinforcing Best Practices to Ensure the Safe and Compliant Transport of Goods in Maritime and Other Forms of Transportation, *available at* https://ofac.treasury.gov/media/932391/download?inline.

[5] *See* Department of the Treasury, Enforcement Release, "OFAC Settles with Toll Holdings Limited for $6,131,855 Related to Apparent Violations of Multiple Sanctions Programs" (Apr. 25, 2022), *available at* https://ofac.treasury.gov/media/922441/download?inline.

apparent violations arose when AL Middle East conspired with Dubai- and Iran-based companies to export storage tank cleaning units from a U.S. company to Iran by falsely listing a Dubai-based company as the end-user on its export documentation. OFAC's investigation revealed that the owner of the Dubai company emailed the sales manager and a senior sales engineer for AL Middle East a memo from an Iranian distributer of oil products, outlining a strategy for procuring U.S.-origin goods from a U.S. company and reexporting them into Iran, while obscuring the ultimate destination of the goods. In effectuating this scheme, AL Middle East willfully caused the U.S. company to export goods indirectly from the United States to Iran in violation of U.S. sanctions.[6]

- In June 2023, Swedbank Latvia AS ("Swedbank Latvia"), a subsidiary of a Sweden-based international financial institution, agreed to pay $3,430,900 to settle its potential civil liability for 386 apparent violations of OFAC sanctions on Crimea. A customer of Swedbank Latvia used Swedbank Latvia's e-banking platform from an internet protocol address in a sanctioned jurisdiction to send payments to persons also located in a sanctioned jurisdiction through U.S. correspondent banks.[7]

The above examples are not an exhaustive list of all fact patterns in which a foreign person might be liable. OFAC will aggressively investigate and pursue such activity in support of high-priority foreign policy objectives.

U.S. Export Control Laws

The U.S. Department of Commerce's Bureau of Industry and Security (BIS) administers and enforces export controls on dual-use and certain munitions items through the Export Administration Regulations (EAR) under the authority of the Export Control Reform Act of 2018 (ECRA). Unlike many other countries, where export-related authorities are limited to direct exports, 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. To put it simply, the law follows the goods.

In addition to the initial export, the EAR also applies to the following:

- **Reexports**, or the shipment of the EAR item from one foreign country to another foreign country and **in-country transfers** (the transfer of an item subject to the EAR within a foreign country);

[6] *See* Department of the Treasury, Enforcement Release, "Alfa Laval Middle East Ltd. Settles Potential Civil Liability for Apparent Violations of the Iranian Transactions and Sanctions Regulations" (July 19, 2021), *available at* https://ofac.treasury.gov/media/911521/download?inline.

[7] *See* Department of the Treasury, Enforcement Release, "OFAC Settles with Swedbank Latvia for $3,430,900 Related to Apparent Violations of Sanctions on Crimea" (June 20, 2023), *available at* https://ofac.treasury.gov/media/931911/download?inline.

- Goods that incorporate a certain percentage of controlled U.S. content (also known as the ***de minimis* thresholds**); and
- Exports from abroad, reexports, and in-country transfers of certain foreign-made items produced using U.S. software, technology, or production equipment (thus subject to a **foreign direct product rule**, or FDPR).

BIS actively enforces U.S. export control laws, regardless of where the offending party is located. Anyone involved in the movement of items subject to the EAR must adhere to U.S. export control laws.

The reach of U.S. export control laws means that parties to an export transaction cannot bypass the EAR by shipping items through a third country. For example, an exporter cannot bypass the U.S. embargo against Iran by shipping an item to a distributor in the United Arab Emirates (UAE) and asking the distributor to transship the item to a customer in Iran. Under U.S. law, this would be considered a reexport to Iran, even though it does not go directly to that country, and both the U.S. exporter and the UAE distributor could be liable for violating U.S. law. Additionally, parties cannot bypass the EAR by changing the end use or end user of an item within a foreign country.[8]

Similarly, foreign parties to an export transaction cannot bypass EAR requirements because the item is located outside the United States and was not shipped directly to the foreign party recipient. For example, a foreign party that has placed an EAR item into inventory that otherwise requires a license to a third country destination if directly exported from the United States generally still must obtain a BIS reexport license prior to shipping to that third country destination.

The EAR may also apply to non-U.S. companies that manufacture items containing U.S.-origin components or software.[9] The factor that determines EAR applicability is the value of the controlled content (*e.g.*, U.S.-origin components, software) within the overall item: If the value exceeds the applicable *de minimis* threshold, it is subject to the EAR. In most situations, a non-U.S.-made item is subject to the EAR if the value of the U.S.-origin controlled content exceeds 25% of the total value of the finished item. For certain destinations (*i.e.*, Cuba, Iran, North Korea, and Syria), the threshold is 10%.[10]

In addition, under the EAR, certain foreign-produced items located outside of the United States that are produced using certain U.S.-controlled technology, software, or production equipment are subject to the EAR when exported from abroad, reexported, or transferred in-country to certain countries or parties on the Entity List. That is, foreign-produced items – even if they never enter the U.S. stream of commerce and no U.S. person is involved in the transaction – may still

[8] *See* 15 C.F.R. § 734.16 (defining transfer (in country)).
[9] *See, e.g.,* 15 C.F.R. § 734.4.
[10] *Id*. at (c) and (d).

be subject to U.S. export control jurisdiction if they meet certain conditions.[11] For example, in May 2020 (as subsequently amended in August 2020), BIS imposed a license requirement through a FDPR for Huawei and its subsidiaries on the Entity List on items that are the direct product of certain U.S.-origin software or technology or produced by a specified plant or major equipment of a plant.[12] BIS also has imposed FDPR controls on certain Chinese entities associated with advanced semiconductors.[13] Similarly, BIS has imposed multiple FDPR controls on certain defense-related entities in Russia and Belarus and certain items destined to Russia, Belarus, and Iran. Given the ubiquity of U.S. semiconductor manufacturing equipment in foreign semiconductor fabrication facilities, these controls generally result in a license requirement for any semiconductor destined to specific entities or locations subject to one of these FDPRs. This means that any semiconductor—no matter where it is produced in the world—may be subject to the FDPR and thus restricted from going to Russia.[14]

BIS Enforcement Actions Against Foreign Companies or Involving Foreign-Produced Items

- On June 9, 2023, BIS issued a Temporary Denial Order (TDO) suspending the export privileges of the Aratos Group, a network of defense-related companies in the Netherlands and Greece, and its president, Nikolaos Bogonikolos, for acting as a procurement network for Russian intelligence services. The TDO is related to a May 22, 2023, criminal indictment issued in the Eastern District of New York and is the result of coordination by the Disruptive Technology Strike Force co-led by the Departments of Justice and Commerce. TDOs are some of the most significant protective measures BIS can issue, cutting off not only the right to export items subject to the EAR from the United States, but also the right to receive or participate in exports from the United States or reexports of items subject to the EAR.

[11] 15 C.F.R. §§ 734.9, 736.2(b)(3).

[12] "Export Administration Regulations: Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule) and the Entity List," 85 Federal Register 29849, May 19, 2020; 85 Fed Reg. 51596 (Aug. 20, 2020).

[13] For more information, *see* "Implementation of Additional Export Controls: Certain Advanced Computing and Semiconductor Manufacturing Items; Supercomputer and Semiconductor End Use; Entity List Modification," 87 Fed. Reg. 62186 (Oct. 13, 2022), *available at* https://www.bis.doc.gov/index.php/documents/federal-register-notices-1/3165-87-fr-62186-advanced-computing-and-semiconductor-manufacturing-items-rule-published-10-13-22/file.

[14] For more information on the Russia and Belarus FDPR, *see* Department of Commerce, "U.S. Department of Commerce and Bureau of Industry and Security Russia and Belarus Fact Sheet" (Feb. 24, 2022), *available at* https://www.commerce.gov/news/fact-sheets/2022/02/us-department-commerce-bureau-industry-and-security-russia-and-belarus.

- As part of its response to Russia's full-scale invasion of Ukraine, BIS imposed expansive controls on the export of aviation-related items to Russia.[15] As a result, any U.S.-origin aircraft or foreign aircraft is subject to a license requirement to fly into Russia if it includes more than 25% controlled U.S.-origin content and is registered in, owned by, controlled by, or under charter or lease by Russia or a national of Russia. Since February 2022, BIS has issued multiple TDOs against foreign airlines—including Nordwind Airlines, Siberian Airlines, and Ural Airlines, among others—for operating U.S. and foreign aircraft subject to the EAR on flights into and out of Russia. BIS also has listed on its website specific aircraft that have violated the Russia controls, including specific Airbus planes that contain more than a *de minimis* amount of U.S.-origin controlled content, such as those operated by Nordwind, Siberian, and Ural Airlines as well as I-Fly, Meridian Air, Red Wings, and Yamal Airlines.[16] The servicing of these planes constitutes a violation of the EAR absent BIS authorization.

- On April 20, 2023, BIS announced a settlement agreement entailing the largest standalone administrative penalty in BIS history: a $300 million penalty against Seagate Technology LLC of Fremont, California (Seagate US) and Seagate Singapore International Headquarters Pte. Ltd., of Singapore (Seagate Singapore) (collectively, Seagate) to resolve allegations that Seagate shipped millions of hard disk drives to Huawei without a license in violation of the Huawei FDPR. Despite the decision by its two main competitors to cease selling to Huawei after the FDPR took effect, Seagate continued to sell and became Huawei's sole source provider for hard disk drives. This case is the first enforcement action and penalty brought under the Huawei FDPR. In addition to the $300 million monetary penalty, Seagate is subject to a suspended five-year denial order that allows BIS to cut off their export privileges if they violate key terms in the settlement agreement.

CRIMINAL ENFORCEMENT OF U.S. SANCTIONS AND EXPORT CONTROL LAWS AGAINST FOREIGN PERSONS AND ENTITIES

The Department of Justice (DOJ) is authorized to bring criminal prosecutions pursuant to IEEPA and ECRA for willful violations of U.S. sanctions and export control laws.[17] Conduct prohibited under these statutes includes "caus[ing] a violation of any license, order, regulation, or prohibition issued" pursuant to IEEPA as well as "caus[ing]" or "induc[ing]" the doing of any act

[15] BIS has also imposed similarly stringent controls on items subject to the EAR that are destined for Belarus.

[16] In total, BIS has determined that 184 aircraft have violated Russia controls. The full list can be found here: https://www.bis.doc.gov/index.php/documents/policy-guidance/3371-2023-10-24-bis-list-of-commercial-and-private-aircraft-potential-ear-violations/file.

[17] *See* 50 U.S.C. § 1705(c); 50 U.S.C. § 4819(b).

prohibited, or the omission of any act required by ECRA or the EAR.[18] Willful violations of either statute are punishable by imprisonment of up to 20 years and a $1 million fine.[19]

In recent months, DOJ has brought charges against multiple foreign-based actors for allegedly seeking to unlawfully transfer U.S.-manufactured technology to prohibited destinations:

- In October 2022, DOJ unsealed an indictment charging three Latvian nationals, one Ukrainian national living in Estonia, one Latvian company, and one Estonian company with violating U.S. export laws and regulations by trying to smuggle from the United States to Russia a dual-use, high-precision computer-controlled grinding machine known as a "jig grinder."[20] As alleged, the defendants conspired to have the Latvian company act as the purported purchaser of the device, and then seek to reexport it from Latvia to a Russian company without first acquiring the requisite license.[21] In carrying out the scheme, the defendants allegedly made false representations to both U.S. and Latvian officials about the destination of the device, which was controlled because of its potential application in nuclear proliferation and defense programs.[22] The jig grinder was intercepted by U.S. authorities in Latvia. Two defendants have pled guilty, and approximately $826,000 was forfeited to the United States.[23] In February 2024, approximately $500,000 of those funds was transferred to the Estonian government for the purpose of providing aid to Ukraine.[24]

- In December 2023, DOJ unsealed an indictment charging one Iran-based person and an individual based in China and Hong Kong for conspiring to illegally purchase and export from the United States to Iran dual-use microelectronics commonly used in UAV production.[25] To obtain the products, the defendants allegedly caused Canadian and French companies to place orders with U.S. manufacturers, causing the items to be shipped first to either Canada and France and then to Hong Kong and China, where they

[18] *See* 50 U.S.C. § 1705(a); 50 U.S.C. § 4819(a)(2)(B).

[19] *See* 50 U.S.C. §1705(c); 50 U.S.C. § 4819(b).

[20] Department of Justice, "Justice Department Announces Charges and Arrests in Two Cases Involving Export Violation Schemes to Aid Russian Military" (Oct. 19, 2022), *available at* https://www.justice.gov/opa/pr/justice-department-announces-charges-and-arrests-two-cases-involving-export-violation-schemes.

[21] Superseding Indictment, ECF No. 1-2, *United States v. Romanyuk*, 3:22-cr-110-VAB (D. Conn., June 2, 2022), ¶ 16.

[22] *Id*.

[23] Department of Justice, "Federal Court Orders Forfeiture of $826K in Funds Used in Attempt to Export Dual-Use High Precision Jig Grinder to Russia" (Apr. 5, 2023), *available at* https://www.justice.gov/opa/pr/federal-court-orders-forfeiture-826k-funds-used-attempt-export-dual-use-high-precision-jig.

[24] Department of Justice, "Justice Department Transfers Approximately $500,000 in Forfeited Russian Funds to Estonia for Benefit of Ukraine" (Feb. 17, 2024), *available at* https://www.justice.gov/opa/pr/justice-department-transfers-approximately-500000-forfeited-russian-funds-estonia-benefit.

[25] Department of Justice, "Iranian National Charged with Unlawfully Procuring Microelectronics Used in Unmanned Aerial Vehicles on Behalf of the Iranian Government" (Dec. 19, 2023), *available at* https://www.justice.gov/opa/pr/iranian-national-charged-unlawfully-procuring-microelectronics-used-unmanned-aerial-vehicles.

were reexported to Iranian end users.[26] The defendants allegedly provided false and misleading information about the ultimate end use and true identities of the end users to the U.S. manufacturers.[27]

- In November 2023, DOJ announced a guilty plea by Binance Holdings Limited, an entity that operated the world's largest cryptocurrency exchange, for various offenses, including violations of U.S. sanctions laws.[28] Binance admitted to knowing that it had a significant number of users from comprehensively sanctioned jurisdictions, such as Iran, as well as a significant number of U.S. users, and Binance further knew that its system would cause U.S. users to transact with users in sanctions jurisdictions.[29] Despite having this awareness, Binance failed to implement controls to prevent trades between U.S. users and users in Iran, resulting in nearly $900 million in trades between users based in the two countries over a four-year period.[30] As part of the plea agreement, which also included admitting to violations of the Bank Secrecy Act, Binance agreed to a $4.3 billion financial penalty.[31] Binance additionally agreed to pay $968,618,825 to settle its potential civil liability for 1,667,153 apparent violations of multiple sanctions programs.[32]

CONCLUSION

Foreign-based companies and individuals are advised to take seriously the impacts of U.S. sanctions and export control laws on their business and operations. Global business organizations and others who participate in international trade should take appropriate steps to understand how these laws may apply to them, what risks are posed by their business operations, and how they can mitigate these risks.

[26] Indictment, ECF No. 1, *United States v. Ardakani, et al.*, 1:20-cr-176-CJN (D.D.C. Sept. 20, 2020), ¶ 23.

[27] *Id*. ¶ 26(E).

[28] Department of Justice, "Binance and CEO Plead Guilty to Federal Charges in $4B Resolution" (Nov. 21, 2023), available at https://www.justice.gov/opa/pr/binance-and-ceo-plead-guilty-federal-charges-4b-resolution.

[29] *Id*.

[30] *Id*.

[31] *Id*.

[32] Department of the Treasury, "OFAC Settles with Binance Holdings, Ltd. for $968,618,825 Related to Apparent Violations of Multiple Sanctions Programs" (Nov. 21, 2023), *available at* https://ofac.treasury.gov/media/932351/download?inline.

COMPLIANCE CONSIDERATIONS FOR FOREIGN-BASED PERSONS

As with any company participating in the global marketplace, foreign-based persons must ensure that they have robust compliance measures in place to avoid violating U.S. sanctions or export control laws. In particular, companies should take care to do the following:

- Employ a risk-based approach to sanctions compliance by developing, implementing, and routinely updating a sanctions compliance program.
- Establish strong internal controls and procedures to govern payments and the movement of goods involving affiliates, subsidiaries, agents, or other counterparties. Such controls can help detect linkages to sanctioned persons or jurisdictions that may otherwise be obscured by complex payment and invoicing arrangements.
- Ensure that know-your-customer information (such as passports, phone numbers, nationalities, countries of residence, incorporation, and operations, and addresses) and geolocation data are appropriately integrated into compliance screening protocols and information is updated on an ongoing basis based on its overall risk assessment and specific customer risk rating.
- Ensure that subsidiaries and affiliates are trained on U.S. sanctions and export controls requirements, can effectively identify red flags, and are empowered to escalate and report prohibited conduct to management.
- Take immediate and effective action when compliance issues are identified, to the extent possible, to identify and implement compensating controls until the root cause of the weakness can be determined and remediated.
- Identify and implement measures to mitigate sanctions and export control risks prior to merging with or acquiring other enterprises, especially where a company is expanding rapidly and/or disparate information technology systems and databases are being integrated across multiple entities.
- Parties who believe that they may have violated sanctions or export control laws should voluntarily self-disclose the conduct to the relevant agency. Please review the Compliance Note: Voluntary Self-Disclosure of Potential Violations.