Guidance to Industry on Iran's UAV-Related Activities

Iran's procurement, development, and proliferation of unmanned aerial vehicles (UAVs) is an increasing threat to international peace and security. The Department of Commerce, the Department of Justice, the Department of State, and the Department of the Treasury are issuing this advisory to alert persons and businesses globally to the threat of Iran's UAV-related activities and the need to take appropriate steps to avoid or prevent any activities that would support the further development of Iran's UAV program.

The United States is committed to countering Iran's UAV programs, including through preventing abuse of the U.S financial system and disrupting the procurement of foreign-sourced components. It is critical that private industry be aware of its legal obligations vis-à-vis entities and items involved in such procurement efforts, given the potential applicability of U.S. export controls and sanctions. The intent of this advisory is to highlight effective due diligence policies, compliance structures, and internal controls relevant specifically to Iran's UAV-related activities to ensure compliance with applicable legal requirements across the entire supply chain. This advisory is also designed to help prevent companies from contributing to Iran's UAV programs, including via direct and indirect transfers to third-country suppliers, which may threaten broader national and international security interests of the United States and its allies and partners.

The Threat

Iran's development, procurement, and proliferation of UAVs destabilizes the Middle East region and beyond. Over the past ten years, Iran has increased its inventory of both armed and unarmed UAVs, whose low cost, simplicity of production, and ease of use make them appealing to entities and countries of concern to which Iran may transfer them, including but not limited to:

Russia: Since at least late August 2022, Iran has transferred hundreds of Shahed- and Mohajer-series UAVs to Russia. Moscow has used these UAVs extensively to strike critical infrastructure during its brutal war of aggression against Ukraine. In October 2022, the United States joined the United Kingdom and France in raising our grave concerns about these transfers from Iran in violation of United Nations (UN) Security Council Resolution 2231. Since then, the United States has continuously worked to expose and disrupt Iran's growing military partnership with Russia, which has helped enable Russia's war of aggression against Ukraine. The European Union and United Kingdom have also sanctioned multiple Iranian individuals and entities involved in Iran's supply of UAVs to Russia.

Houthis: Iran has continued its destabilizing activities in Yemen, including sending illicit shipments of UAVs and other weapons to the Houthis, who have used them to conduct strikes inside Yemen and on neighboring countries, Saudi Arabia, and the United Arab Emirates.

Overseas Production Facilities: Reports indicate Iran has offered to provide UAV production technology and facilities to Tajikistan and Russia. With these efforts, Tehran may be seeking to strengthen bilateral relationships, boost the profits of its export sector, and complicate efforts to constrain its UAV activities through export controls and other measures.

Key Items

Iran relies on foreign procurement to obtain items it cannot produce domestically, often preferring U.S.-origin technologies. Recovered Iranian-origin UAVs used by Russian forces in Ukraine reveal that Iran's UAV program has used many components produced by third-country suppliers. Industry should be aware of its compliance obligations due to the threat posed by the extensive overseas network of procurement agents, front companies, suppliers, and intermediaries Iran uses to obtain UAV components, all of which employ a variety of methods to evade export controls and sanctions. Industry should exercise extra vigilance due to the ubiquitous nature of many of the items, as Iran utilizes commercial-grade components in its weapons.

The following list highlights key commodities sought by Iran for its development of UAVs.

Electronics, such as transceiver modules, processors and controllers, memories, amplifiers, and other electronic integrated circuits. Most notably, Iran relies on certain U.S.-branded items such as field programmable gate arrays (FPGAs), RF transceivers, microcontrollers, and capacitors. Some of these are low-technology items and may not be included on the Commerce Control List (CCL)[1] of the Export Administration Regulations (EAR, 15 C.F.R. Parts 730-774) (*i.e.*, they are designated as "EAR99") but nonetheless may be controlled for export to Iran under U.S. sanctions or export controls.

Guidance, Navigation and Control Equipment, such as accelerometers, gyroscopes, inertial measurement units (IMUs), and other navigational sensors.

Components, such as aircraft spark-ignition and compression-ignition internal combustion piston engines and associated spare parts, and modules such as flight computers.

[1] 15 C.F.R. Part 774, Supplement No.1

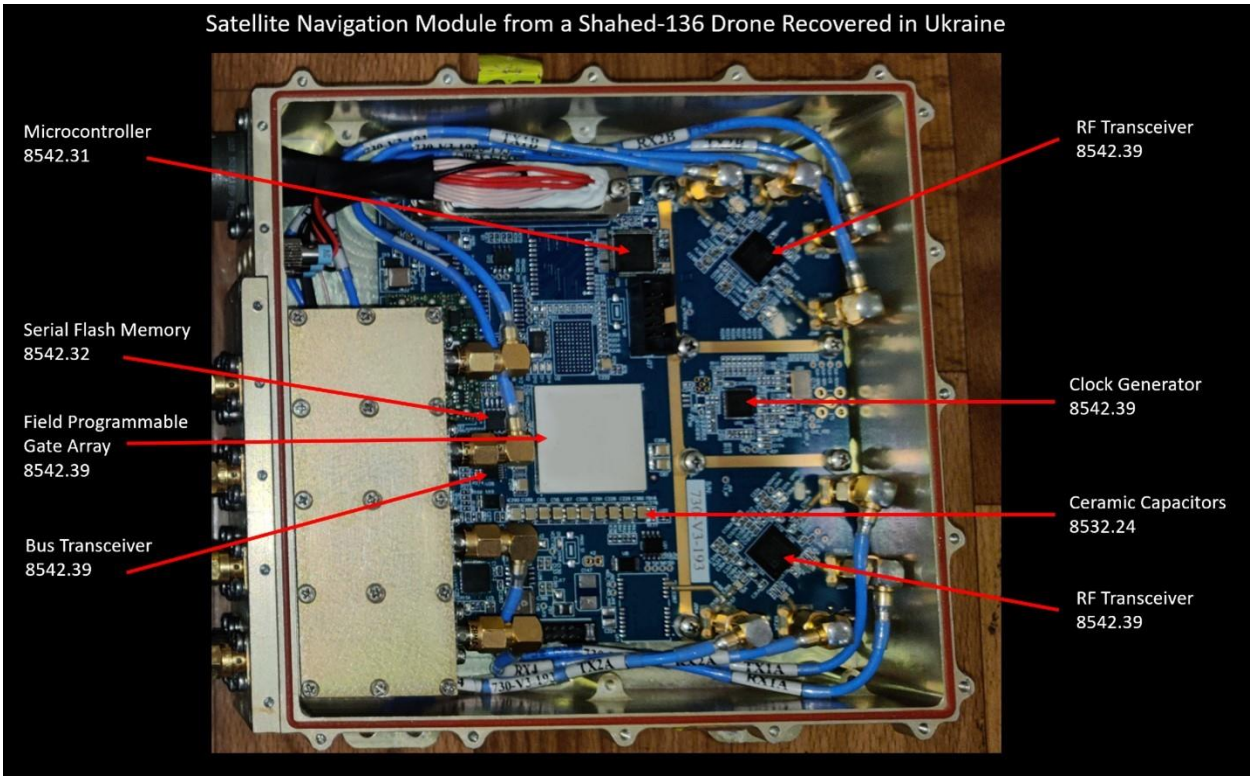

Figure 1. Recovered Iranian UAV containing components classified under harmonized tariff schedule codes listed in supplement no. 7 to 15 CFR part 746 (see section on U.S. Export Controls below)

Exporters, manufacturers, and distributors of items listed above should be aware of the importance of carrying out customer due diligence in a way consistent with BIS's *"Know Your Customer" Guidance and Red Flags*[2], and should track to whom they are selling and/or shipping their items. We urge manufacturers that supply UAV-relevant items to establish multiple methods to track such items due to the observed prevalence of methods used to obscure the sources of components found in Iranian UAVs, such as the lasering off of serial numbers and other identifying information.

U.S. Export Controls

The United States has long regulated the export of UAVs and related items via a range of controls, including license requirements for items listed on the United States Munitions List, as set forth in the International Traffic in Arms Regulations (ITAR)[3] and for items listed on the Commerce Control List (CCL).[4] The United States also imposes catch-all controls on items that could contribute to certain UAV systems, even if they are not described on the CCL.

Building on these pre-existing controls, BIS has issued several rules that target Iran's supply of UAVs to Russia to enhance Russia's defense industrial base and its military efforts against

[2] *See* 15 C.F.R. Part 732, Supplement No. 3.
[3] 22 C.F.R. § 121.1.
[4] *Supra* note 1.

Ukraine. On February 24, 2023, BIS amended[5] the EAR (15 CFR 746.7) to impose additional licensing requirements on certain EAR99 items destined to Iran—regardless of whether the transaction originates in the United States, or whether a U.S. person is involved.[6] In that same rule, BIS established a new list (Supplement No. 7 to part 746) to identify these EAR99 items, including certain engines, navigational equipment, and electronics, by Harmonized Tariff Schedule (HTS) 6 Code[7], and also imposed license requirements on certain foreign-produced items that met these descriptions. On May 19, 2023, BIS again amended the EAR to add additional electronic components to Supplement No. 7 to part 746 of the EAR.[8]

BIS has also created a new Foreign Direct Product (FDP) Rule specific to Iran[9] for items in certain categories of the Commerce Control List (CCL) covering electronics, computers, communications and information security, and navigation and avionics, as well as the EAR99 items identified in Supplement No. 7 to Part 746. As a result of this new FDP Rule, exporters require a U.S. Government authorization for transfer of these items when produced outside the United States with certain U.S. technology, software, or production equipment when exports are destined to Iran or for use in connection with certain equipment destined to Iran, even when such items were never exported from the United States and/or no U.S. person is involved in the transaction. BIS also expanded the existing Russia and Belarus FDP rule to cover EAR99 items in Supplement. No. 7.[10]

BIS has also added numerous entities to the Entity List for their involvement in the production of Iranian UAVs, or in the transfer of UAVs from Iran to Russia, most notably on February 1[11] and April 17, 2023. [12] As a result of these actions, a BIS license is required to export, reexport, or transfer (in-country) any item subject to the EAR when the listed entity is a party to the transaction. BIS has adopted a policy of denial for all such license applications. Further, BIS and the Department of the Treasury's Financial Crimes Enforcement Network (FinCen) have issued guidance for financial institutions on the typologies regarding the use of the financial system to evade export controls.

---

[5] Export Control Measures Under the Export Administration Regulations (EAR) To Address Iranian Unmanned Aerial Vehicles (UAVs) and Their Use by the Russian Federation Against Ukraine, 88 Fed. Reg. 12,150 (Feb. 27, 2023), *available at*: https://www.federalregister.gov/documents/2023/02/27/2023-03930/export-control-measures-under-the-export-administration-regulations-ear-to-address-iranian-unmanned.

[6] 15 C.F.R. § 746.7.

[7] 15 C.F.R. Part 746, Supplement No. 7.

[8] Implementation of Additional Sanctions Against Russia and Belarus Under the Export Administration Regulations (EAR) and Refinements to Existing Controls, 88 Fed. Reg. 33,422 (May 23, 2023), *available at*: https://www.federalregister.gov/documents/2023/05/23/2023-10774/implementation-of-additional-sanctions-against-russia-and-belarus-under-the-export-administration.

[9] 15 C.F.R. § 734.9(j).

[10] 15 C.F.R. § 734.9(f)

[11] Additions to the Entity List, 88 Fed. Reg. 6,621 (Feb. 02, 2023), *available at:* https://www.federalregister.gov/documents/2023/02/01/2023-02130/additions-to-the-entity-list.

[12] Additions and Revisions of Entities to the Entity List, 88 Fed. Reg. 23,332 (Apr. 17, 2023), *available at* https://www.federalregister.gov/documents/2023/04/17/2023-07840/additions-and-revisions-of-entities-to-the-entity-list.

HTS–6 codes	HTS description
840710	Aircraft spark-ignition reciprocating or rotary internal combustion piston engines.
840890	Compression-ignition internal combustion piston engines (diesel or semi-diesel engines), NESOI.
840910	Parts for spark-ignition or rotary internal combustion piston engines or compression-ignition internal combustion piston engines, for aircraft.
847150	Processing units other than those of subheading 8471.41 or 8471.49, whether or not containing in the same housing one or two of the following types of unit: storage units, input units, output units.
851762	Machines for the reception, conversion and transmission or regeneration of voice, images or other data, including switching and routing apparatus.
852691	Radio navigational aid apparatus.
853221	Tantalum capacitors.
853224	Fixed capacitors NESOI, multilayer ceramic dielectric.
854231	Processors and controllers, whether or not combined with memories, converters, logic circuits, amplifiers, clock and timing circuits, or other circuits.
854232	Memories.
854233	Amplifiers.
854239	Other electronic integrated circuits.
854800	Electrical parts of machinery or apparatus, NESOI

Figure 2. Supplement 7 HTS-6 Codes

U.S. Sanctions

Through the Department of the Treasury's Office of Foreign Assets Control (OFAC), the United States administers and enforces a comprehensive trade embargo against Iran as set forth in the Iranian Transactions and Sanctions Regulations, 31 C.F.R. Part 560 (ITSR). The ITSR generally prohibits most direct or indirect commercial, financial, or trade transactions with Iran by U.S. persons or within the United States, unless authorized by OFAC or exempted by statute. Furthermore, under the ITSR, U.S. persons are generally prohibited from engaging in any transaction or dealing involving the Government of Iran or Iranian financial institutions and are obligated to block the property and interests in property of such persons if they come within a U.S. person's possession or control, unless the transactions are exempt or authorized by OFAC.

Under the ITSR, non-U.S. persons are prohibited from reexporting from a third country, directly or indirectly, any goods, technology, or services that have been exported from the United States,

if (1) undertaken with knowledge or reason to know that the re-exportation is intended specifically for Iran or the Government of Iran, and (2) the item is subject to U.S. export licensing requirements. This prohibition applies to the re-exportation by non-U.S. persons of foreign-made items with 10 percent or more U.S.-controlled content by value. Non-U.S. persons may also violate the ITSR by directly or indirectly exporting services from the United States, or by causing other persons to violate U.S. sanctions against Iran. For example, a non-U.S. person that processes a U.S. dollar-denominated transaction through a U.S. financial institution pertaining to the unauthorized procurement, sale, delivery, or provision of goods or services to Iran or the Government of Iran could be subject to an enforcement action by OFAC, even if the transaction is otherwise conducted wholly outside of the United States.

Separately, persons who provide material support to certain designated persons on the List of Specially Designated Nationals and Blocked Persons (SDN List)[13] could be subject to sanctions and added to the SDN List. Furthermore, foreign financial institutions that knowingly conduct or facilitate significant financial transactions for or on behalf of certain designated persons may be exposed to sanctions, which may include designation and listing on the SDN List or restrictions on or loss of access to the U.S. financial system.

In addition, the United States has designated under several other sanctions authorities, including Executive Order (E.O.) 13382 and E.O. 14024, numerous Iranian entities and individuals involved in the production, procurement, and proliferation of UAV systems, as well as third-country entities (including in Russia, China, and Türkiye) involved in either the receipt of Iranian UAVs or the supply of UAV components to Iran. During the last 12 months, the United States has designated the following Iranian persons for engaging in certain activities related to the development, procurement, and proliferation of UAVs and UAV components:

UAV Production and Development: The United States has designated Qods Aviation, Shahed Aviation, Paravar Pars Company, Design and Manufacturing of Aircraft Engines (DAMA), Baharestan Kish Company, and Shahed Aviation Industries Research Center (SAIRC).

UAV Component Procurement: The United States has designated Defense Technology and Science Research Center (DTSRC), Farazan Industrial Engineering, Inc., and Selin Technic Co.

UAV Proliferation: The United States has designated Safiran Airport Services.

List of Targeting Provisions in Certain Sanctions Authorities

The United States and the United Nations (UN) have created multiple sanctions regimes that address the procurement and proliferation of UAVs and related components, technology, and materials by, to, and from Iran. Industry should be aware of the following non-exhaustive list of targeting provisions contained in certain mandatory and discretionary authorities that may apply:

The Iran, North Korea, and Syria Nonproliferation Act (INKSNA) requires reports to Congress periodically on every foreign person for whom there is credible information indicating that the

[13] List of Specially Designated Nationals and Blocked Persons (SDN List), *available at:* https://ofac.treasury.gov/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists

foreign person transferred to/acquired from Iran, Syria, or North Korea certain items (mostly items controlled for export by the Missile Technology Control Regime (MTCR) and other multilateral regimes). INKSNA also authorizes the imposition of sanctions on the persons included in the report. Sanctions include a U.S. Government procurement ban, U.S. Government assistance ban, an import ban, and a ban on the export or reexport of dual-use items and munitions to sanctioned entities.

Section 73 of the Arms Export Control Act and Section 11B(b)(1) of the Export Administration Act of 1979[14] authorizes imposition of sanctions against foreign persons determined to have knowingly transferred MTCR Annex items that contribute to the acquisition, design, development, or production of missiles in a non-MTCR country. These authorities specify different consequences based on the nature of the items transferred but may involve a denial of U.S. Government contracts or export licenses or an import ban.

E.O. 12938 authorizes sanctions against any foreign persons determined to have engaged, or attempted to engage, in activities that materially contributed, or posed a risk of materially contributing, to the proliferation of WMD or their means of delivery.

E.O. 13382 authorizes blocking sanctions against any foreign persons determined to have engaged, or attempted to engage, in activities or transactions that have materially contributed to, or pose a risk of materially contributing to, the proliferation of WMD or their means of delivery (including missiles capable of delivering such weapons) by a foreign person or country of proliferation concern. The E.O. also provides discretion to block any foreign persons determined to have provided financial or material assistance, or goods or support for, or to be owned or controlled by, any entity already blocked under this E.O.

E.O. 13949 authorizes blocking sanctions on persons determined to have engaged in activities that materially contribute to the transfer of arms and related materiel to or from Iran as well as on persons that have engaged or attempted to engage in activities that materially contribute or pose a risk of materially contributing to the proliferation of arms or related materiel by the Government of Iran or paramilitary organizations supported by it. It also provides for sanctions on those who support or who act for or on behalf of persons who are blocked under the E.O.

Iran Freedom and Counterproliferation Act (IFCA) requires the imposition of sanctions on persons determined to have engaged in the sale, supply, or transfer to or from Iran of precious and certain other metals, graphite, coal, and industrial software; the provision of underwriting services, insurance, or reinsurance to activities and persons targeted by U.S. sanctions against Iran; and financial transactions on behalf of sanctioned Iranian individuals and entities.

Countering America's Adversaries Through Sanctions Act (CAATSA) Section 107 authorizes sanctions against any person determined to knowingly engage in any activity that materially contributes to the supply, sale, or transfer directly or indirectly to or from Iran, or for the use in or benefit of Iran, of any battle tanks, armored combat vehicles, large caliber artillery systems, combat aircraft, attack helicopters, warships, missiles or missile systems, as defined for the

[14] Section 73 of the Arms Export Control Act and Section 11B(b)(1) of the Export Administration Act of 1979, consistent with section 176(b) of Public Law 115-232, the Export Control Reform Act (50 U.S.C. 4601 note.

purpose of the UN Register of Conventional Arms, or related materiel, including spare parts; or knowingly provides to Iran any related technical training, financial resources or services, advice, other services or assistance. Combat aircraft are defined by the UN as "a fixed-wing or variable-geometry aircraft armed and equipped to engage targets by employing guided missiles, unguided rockets, bombs, guns, cannons, or other weapons of destruction," which includes armed UAVs.

UN Security Council Resolution 2231 prohibits the sale, supply, or transfer to or from Iran (absent the UN Security Council's advance permission on a case-by-case basis) of items controlled by the Missile Technology Control Regime – which includes Shahed- and Mohajer-series UAVs. The provisions of Resolution 2231 covering missile activity will remain in force until October 18, 2023.

More information about these authorities can be found at the appropriate Department of State, Department of the Treasury, and/or, UN websites. Depending on the details of the transaction, other authorities such as E.O. 14024 (which, among other things, provides authority to block any foreign persons determined to operate or have operated in specified sectors of the Russian Federation economy) and UN Security Council Resolution 2216 (which imposes a targeted arms embargo on Yemen), may also apply.

Select Red Flag Indicators of Export Control Evasion

The U.S. Government expects companies to have effective and comprehensive compliance programs that detect efforts by individuals or entities to evade or otherwise violate sanctions and export controls.

Effective compliance programs employ a risk-based approach to sanctions and export controls by developing, implementing, and routinely updating compliance measures. Companies such as manufacturers, distributors, resellers, and freight forwarders are often best positioned to determine whether a particular transaction or inquiry is consistent with industry norms and practices, and otherwise indicates an elevated risk of sanctions or export control evasion. Companies should exercise heightened caution and conduct additional due diligence if they detect warning signs of potential sanctions or export control violations.[15]

Compliance programs should reflect management commitment to compliance and include risk assessment, internal controls, testing, auditing, and training. [16] Effective programs empower and equip staff to identify and report potential violations of U.S. sanctions and export controls to compliance personnel so that companies can prevent or cease violative conduct and determine whether to make timely voluntary disclosures to the U.S. Government. Optimally, compliance programs should include controls tailored to the risks the business faces, such as diversion by third-party intermediaries.

---

[15] For more information on voluntary self-disclosures, see https://www.bis.doc.gov/index.php/enforcement/oee/voluntary-self-disclosure.

[16] https://ofac.treasury.gov/media/16331/download?inline
https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file

While not exhaustive, the "red flags" listed below demonstrate that a party to the transaction may be engaged in efforts to evade or otherwise violate sanctions or export controls:

- Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure (i) ownership, (ii) source of funds, or (iii) countries/entities involved, particularly sanctioned jurisdictions or restricted entities;
- Reluctance to share information about the end use of a product, including reluctance to complete an end-user form;
- Declining customary installation, training, or maintenance of the purchased item(s);
- "Cyber spoofing" of email or web addresses to give the appearance that an illegitimate inquiry is coming from a legitimate business. Often these attempts will leverage known business relationships to lend credibility to the spoofing attempt.
- Internet or corporate website traffic originating from IP addresses that do not correspond to a customer's reported location data;
- Transactions involving entities with little or no web presence;
- Use of personal rather than corporate email addresses;
- Last-minute changes to shipping instructions that appear contrary to customer history or business practices;
- Payment coming from a third-party country or business not listed on the End-User Statement or another applicable end-user form;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Changes to standard business documents that obscure the ultimate customer;
- Operation of businesses using residential addresses or addresses found to be common to multiple corporate entities;
- Transactions involving the use of freight-forwarding firms[17] or other mail forwarding addresses listed as the product's ultimate customer address;
- Transactions associated with atypical shipping routes for a product and destination; or,
- Routing purchases through certain transshipment points commonly used to illegally redirect restricted items to embargoed destinations.

Further, companies should be aware that customers that use complex sales and distribution models may hinder visibility into the ultimate end-users of their technology, services, or products.

Best practices in the face of such risks may include screening current and new customers, intermediaries, and counterparties through the Consolidated Screening List maintained by the Department of Commerce and the SDN List maintained by the Department of the Treasury, as well as conducting risk-based due diligence on customers, intermediaries, and counterparties. Companies should also regularly consult guidance and advisories from the Department of State, Department of the Treasury, and the Department of Commerce to inform and strengthen their compliance programs.

[17] A freight forwarder is a person or company that loads, or charters and loads, any form of transport or a person whose business is to receive and forward goods. The goods are often sent in a container for multimodal transport. See generally BIS, Freight Forwarder Guidance.

Penalties for Violations of Sanctions and Export Controls; Enforcement Actions

Department of the Treasury: U.S. persons or foreign persons over which OFAC exercises jurisdiction can face significant monetary penalties in addition to other enforcement action for conduct in violation of OFAC's regulations. Failure to comply with U.S. sanctions regulations can result in civil and criminal penalties under U.S. law. For information about developing and maintaining a sanctions compliance program, please see *A Framework for OFAC Compliance Commitments*. Companies with questions about their sanctions compliance obligations may contact OFAC at OFAC_feedback@treasury.gov or 1 (800) 540-6322.

Department of Commerce: Persons who violate export controls under the EAR may face administrative or criminal enforcement action. BIS investigators work with analysts to detect, disrupt, and dismantle facilitation networks supporting Iran. As set forth in the Export Reform Act of 2018 (ECRA), 50 U.S.C. 4801-4852, maximum criminal penalties can reach 20 years' imprisonment and up to $1 million in fines per violation, or both. Current administrative monetary penalties are the greater of $353,534 or twice the value of the transaction per violation and/or the denial of export privileges. BIS may also temporarily deny a domestic or foreign party's export privileges upon a showing that such denial is necessary to prevent an imminent violation of the EAR. Furthermore, BIS has the authority under Section 1760(e) of ECRA to deny for up to 10 years the export privileges of parties convicted of certain crimes, including violations relating to U.S. sanctions against Iran. BIS may also add foreign parties to its Entity List for activities such as providing assistance to Iran's procurement activities or weapons program. BIS lists foreign persons, businesses, research institutions, government, and private organizations on its Entity List that have been determined to be acting contrary to U.S. national security and foreign policy interests. These parties generally require a license to receive most items subject to the EAR, and license applications are generally subject to a review policy of a presumption of denial. The availability of license exceptions is limited. The license requirement applies to exports, reexports, and in-country transfers involving the listed party. BIS also can suspend the availability of license exceptions for foreign parties on the Unverified List if an end-use check cannot be completed. A list of individuals and entities that have been denied export privileges or placed on one of the BIS restricted party lists may be found in the CSL.

Department of Justice: The Department of Justice (DOJ) investigates and prosecutes criminal violations of U.S. sanctions and export control laws, including the Export Control Reform Act of 2018 ("ECRA"), 50 U.S.C. §§ 4801-52, and the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-09. Willful violation of either statute is punishable by up to 20 years in prison and a penalty of up to $1 million. DOJ has successfully prosecuted multiple defendants for willfully violating these statutes in connection with their efforts to export UAV-related goods to Iran, including the following recent actions:

- In January 2022, a UK national pled guilty to violating IEEPA and the ITSR as part of a conspiracy to attempt to export to Iran multiple types of items with both commercial and military uses. Among those items was a counter-drone system that can be used to

stop, identify, redirect, land, or take control of a targeted UAV. The UK national is scheduled to be sentenced in September 2023.[18]

- In August 2018, a Canadian national was sentenced to 42 months in prison for illegally exporting and conspiring to export to Iran various types of items, including two types of thermal imaging cameras that can be used in military drones. The defendant used front companies in China and co-conspirators in Iran, Türkiye, and Portugal to try to evade U.S. laws.[19]

In addition, DOJ is leading two interagency law enforcement initiatives that will help undermine Iran's ability to acquire UAV technology. DOJ leads Task Force KleptoCapture, which was stood up in March 2022 to enforce the sanctions, export controls, and other economic countermeasures imposed on Russia for its unprovoked military invasion of Ukraine. One of the central goals of the Task Force is to cut off support to Russia's war effort, including the transfer of UAVs from Iran that are being used against the Ukrainian people.[20] In February 2023, DOJ and BIS created the Disruptive Technology Strike Force, an interagency effort focused on investigating and prosecuting the illicit transfer of sensitive technologies to foreign state adversaries, including Iran.[21]

In March 2023, DOJ's National Security Division (NSD) issued an updated voluntary self-disclosure policy that underscores the imperative that companies voluntarily disclose potential criminal violations of U.S. national security laws, including sanctions and export control laws, or face criminal exposure.[22] As set forth in NSD's Enforcement Policy for Business Organizations, where a company voluntarily discloses potentially criminal violations, fully cooperates, and takes timely and appropriate remedial steps, and where there are no aggravating factors, there will be a presumption that the company will receive a non-prosecution agreement and will not pay a fine. By contrast, where a company's conduct causes an elevated threat to national security, a stricter penalty may be warranted. In furtherance of these efforts to crack down on corporate non-compliance with national security laws, DOJ also announced the hiring of 25 new prosecutors to investigate and prosecute sanctions evasion, export control violations, and similar economic crimes.[23]

---

[18] U.S. Department of Justice, "Indictment and Guilty Plea Entered in Iranian Export Case" (Jan. 27, 2022), *available at* https://www.justice.gov/opa/pr/indictment-and-guilty-plea-entered-iranian-export-case.

[19] U.S. Department of Justice, "Canadian Sentenced to 3+ Years in Prison for Conspiracy to Export Restricted Goods and Technology to Iran" (Aug. 22, 2018), *available at* https://www.justice.gov/opa/pr/canadian-sentenced-3-years-prison-conspiracy-export-restricted-goods-and-technology-iran.

[20] Information about the Task Force's accomplishments in the first year following Russia's invasion of Ukraine is available here: https://www.justice.gov/opa/press-release/file/1569781/download.

[21] U.S. Department of Justice, "Justice and Commerce Departments Announce Creation of Disruptive Technology Strike Force" (Feb. 16, 2023), *available at* https://www.justice.gov/opa/pr/justice-and-commerce-departments-announce-creation-disruptive-technology-strike-force.

[22] NSD Enforcement Policy for Business Organizations, *available at* https://www.justice.gov/media/1285121/dl?inline=.

[23] Deputy Atty. Gen. Lisa Monaco, Remarks at Am. Bar Assoc. Nat'l Inst. on White Collar Crime (March 2, 2023), *available at* https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-monaco-delivers-remarks-american-bar-association-national.