Buchanan

Navigating the Law:
Economic Sanctions and Export Controls Handbook

By Daniel B. Pickard, Shareholder, Chair,
International Trade & National Security Practice Group

February 2024

Expanded sanctions and export control regimes have re-emerged as a key component of U.S. national security and foreign policy reflecting a current era of increased global interconnectedness and federal regulators promising "big-ticket" enforcement actions. Federal agencies have recently begun imposing sanctions and export controls of unprecedented scope and scale, and the U.S. Department of Justice is actively prosecuting those entities and individuals who violate the same. Therefore, U.S. and multinational companies must be vigilant in their compliance efforts.

ECONOMIC SANCTIONS: THE BASICS

U.S. Sanctions Regimes

Economic sanctions, primarily administered and enforced by the U.S. Department of Treasury, Office of Foreign Assets Control (OFAC), play a vital role in U.S. national security policy. Generally, OFAC sanctions prohibit individuals/entities from doing business with or engaging in financial transactions involving, directly or indirectly, a sanctioned (or "blocked") person/entity.

This prohibition applies, even if such person is acting on behalf of an organization which is not the subject of sanctions, unless authorized by OFAC or expressly exempted by statute.

OFAC's prohibitions are broad and include imports as well as exports of goods, technology, or services, and attempts to facilitate any of the same – such as approving or "clearing" a transaction involving a sanctioned party.

Categories of Sanctions

U.S. sanctions generally fall into four categories: (1) country-based or comprehensive sanctions (also known as “embargoes”); (2) targeted sanctions against identified individuals and/or entities (also known as “smart sanctions”); (3) sectoral sanctions; and (4) secondary sanctions.

- Comprehensive Sanctions: Comprehensive sanctions programs, or embargoes, generally prohibit all trade by individuals and/or entities subject to U.S. jurisdiction with specific countries or regions. Currently, the United States levies country-based sanctions against: Cuba, Iran, North Korea, Syria and the Crimea Region of Ukraine. As such, individuals and entities subject to U.S. jurisdiction are prohibited from doing business with organizations and/or individuals within these countries/regions, as well as the countries themselves, unless authorized by OFAC, either via a license or exemption.

- Targeted Sanctions: Also known as “smart” sanctions, OFAC maintains targeted sanctions against individuals and entities owned or controlled by, or acting for or on behalf of, countries subject to the various U.S. sanctions regimes or who have been judged to be engaged in actions that endanger or undermine U.S. foreign policy or national security objectives. Individuals and entities subject to targeted sanctions are identified on OFAC’s Specially Designated Nationals and Blocked Persons List (SDN List).

- Sectoral Sanctions: OFAC also administers certain sectoral sanctions, which target specific sectors of a sanctioned country or regime’s economy. For example, OFAC identifies persons operating in sectors of the Russian economy, identified by the Secretary of Treasury as being subject to sanctions in its publication the Sectoral Sanctions Identifications (SSI) List. Directives found within the SSI describe specific prohibitions on dealings with the persons/entities identified. Other countries, such as Burma (Myanmar) and Yemen, are subject to OFAC sanctions for transactions related to activities of specific political/social parties operating within these countries.

- Secondary Sanctions: Secondary sanctions, a relatively new regime, target non-U.S. persons, primarily foreign financial institutions and sanctions evaders, who do business with entities subject to other U.S. sanctions regimes. Secondary sanctions are designed to prevent third parties from doing business with countries subject to separate sanctions regimes and rely heavily on the significance of the U.S. financial system and U.S. dollar.

OFAC Jurisdiction

OFAC’s jurisdiction extends to all U.S. persons, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches.

Additionally, OFAC can assert jurisdiction over foreign individuals, entities and categories of transactions, including correspondent banks which utilize the U.S. central banking system, transactions with a denominated in U.S. dollars and foreign persons in possession of U.S-origin products.

Further broadening its jurisdiction, OFAC utilizes a "50 Percent Rule." The Rule imposes sanctions on entities that have one or more blocked persons owning 50% or more of the entity (directly or indirectly) in the aggregate. OFAC urges organizations considering a potential transaction to conduct appropriate due diligence on entities that are party to or involved with the contemplated transaction or with which account relationships are maintained in order to determine relevant ownership stakes. Certain actors are now turning to third-party intermediaries and transshipment points to circumvent restrictions, adding even more complexity to the sanctions regulatory regime.

OFAC Licenses

OFAC licenses are, generally, authorizations to engage in a transaction that otherwise be prohibited pursuant to OFAC sanctions regimes. Persons engaging in transactions pursuant to general or specific licenses must ensure that all conditions of the license(s) are strictly observed.

- General Licenses: General licenses from OFAC authorize a particular type of transaction for a class of persons which would otherwise be prohibited under the relevant sanctions regime. Where a general license is applicable, the individual/entity looking to participate in such a transaction is not required to seek a specific license.
- Specific Licenses: A specific license is a written document issued by OFAC to a particular person or entity, authorizing a particular transaction in response to a written license application. In order to obtain a specific license, individuals/entities may submit a written license application to OFAC providing the details of the contemplated transaction and requesting authorization to engage in the same.

Exceptions to OFAC Sanctions

While each OFAC sanctions regime provides exceptions to its general prohibitions, the contours of each specific exception/exemption are nuanced and fact specific. As such, it is vitally important for individuals and organizations, if they seek to take advantage of an exception, to thoroughly review its requirements, often with the assistance of outside counsel, and to document its applicability to the specific factual circumstances at issue.
Included in the various sanctions programs, are certain important humanitarian exceptions of which non-profit organizations and others should be aware. These include exceptions for: (1) official business of the U.S. government; (2) official business of

certain international organizations and entities, such as the United Nations or International Red Cross; (3) certain humanitarian transactions in support of nongovernmental organizations' activities, such as disaster relief and health services; and (4) the provision of agricultural commodities, medicine, and medical devices, including replacement parts, components, and software updates for medical devices, for personal, non-commercial use.

Voluntary Self-Disclosure

OFAC encourages individuals/entities to make voluntary self-disclosures of a potential violation of a sanctions regime When disclosures are made, individuals/entities need to provide for the possibility of a mitigated penalty if/when a violation is found. Self-disclosing potential violations can provide significant mitigation of civil or criminal liability, the extent of which depends on the agency, including potential non-prosecution agreements or a reduction in the base penalty amount for civil or criminal penalties. Thus, companies or individuals that suspect a potential violation of an OFAC sanctions program should engage with outside counsel to consider voluntary self-disclosure as soon as possible.

Potential Penalties for Non-Compliance with OFAC Sanctions

OFAC sanctions are a "strict liability" regime, meaning individuals and entities may be subject to civil liability for sanctions violations regardless of whether they intended to violate any specific statute or regulation. Civil penalties for violations of OFAC's sanctions regulations may include but shall not exceed: (1) $350,000 per violation, or (2) an amount which is twice the amount of the transaction that is the basis of the violation which led to the imposition of the penalty.

Where individuals and/or entities "willfully" commit sanctions violations, criminal penalties, upon conviction, may include, but shall not exceed: (1) $1,000,000 per violation, (2) if a natural person, imprisonment for not more than twenty (20) years, or (3) both (1) and (2).

In addition to civil and criminal penalties for violations of sanctions regulations, OFAC utilized various regulatory enforcement/compliance mechanisms, including:

- Request(s) for Additional Information: Pursuant to regulatory authority, OFAC may request additional information from individuals/entities to determine whether a violation of sanctions regulations has occurred. Like administrative subpoenas from other federal agencies, OFAC's requests for additional information may become the subject of judicial enforcement.

- Cautionary Letter: A cautionary letter indicates that OFAC has not found sufficient evidence to establish a violation of sanctions regulations or has determined that a penalty is unwarranted under the specific circumstances.

- Finding of Violation: OFAC may issue a finding of violation where it determines that a violation of sanctions regulations has occurred but that a civil or criminal penalty is not the most appropriate response. Findings of violations often increase the possibility that the subject of the violation could face civil or criminal penalties for continued violations.

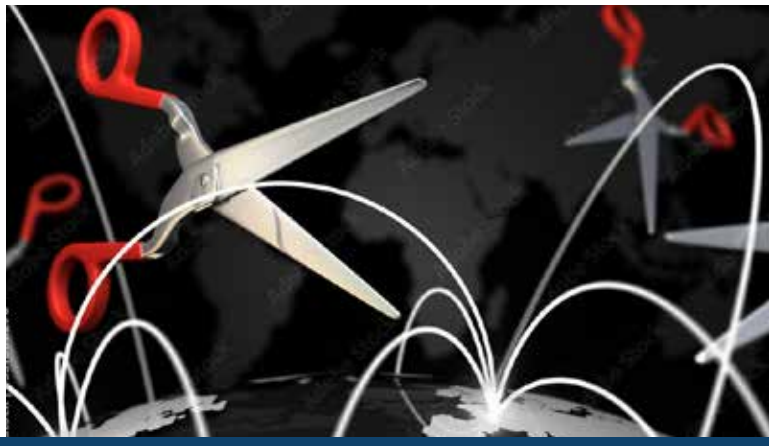
- Administrative Action: In certain circumstances, OFAC, rather than seeking civil or criminal enforcement, will take administrative action in the form of a cease-and-desist letter. OFAC may also take action against an individual/entity's license or license application, including denial, suspension, modification or revocation.

Recent Enforcement Actions

- *United States v. Binance:* In November 2023, the Department of Treasury announced its largest settlement in history against Binance Holdings Ltd. and its affiliates (collectively, "Binance"), including a settlement with OFAC in the amount of $968 million. Binance is the world's largest virtual currency exchange, responsible for an estimated 60% of centralized virtual currency spot trading. As detailed in the settlement agreement, OFAC found that between August 2017 and October 2022, Binance executed more than 1.67 million virtual currency trades on its Binance.com platform between U.S. persons and users in sanctioned jurisdictions and blocked persons. Additionally, OFAC found that Binance deliberately undermined and ineffectually implemented its own sanctions compliance controls.

- *United States v. PURE:* In December 2023, an insurance organization based in White Plains, New York, that primarily offers insurance policies and coverages for luxury homes, automobiles, art collections, jewelry, and watercraft, agreed to pay $466,200 to settle its potential civil liability for 39 apparent violations of OFAC's Ukraine/Russia-related sanctions. OFAC found that between May 2018 and July 2020, Privilege Underwriters Reciprocal Exchange (PURE) engaged in transactions involving a blocked Panama-based company owned by Specially Designated National Viktor Vekselberg. OFAC announced that its settlement amount reflected its determination that the organization's apparent violations were not voluntarily self-disclosed.

- *United States v. Poloniex:* In May 2023, OFAC announced a settlement with Poloniex, LLC. Poloniex agreed to pay $7.6 million to settle its potential civil liability for violations of sanctions against Crimea, Cuba, Iran, Sudan, and Syria. According to OFAC, between January 2014 and November 2019, the Poloniex trading platform allowed customers located in sanctioned jurisdictions to engage in online digital asset-related transactions — consisting of trades, deposits, and withdrawals — with a combined value of $15 million, despite having reason to know their location based on both Know Your Customer (KYC) information and internet protocol (IP) address data. The settlement amount reflects OFAC's determination that Poloniex's apparent violations were not voluntarily self-disclosed.



EXPORT ADMINISTRATION REGULATIONS (EAR): THE BASICS

U.S. international trade and national security policy includes a long history of establishing export control regimes to monitor, manage, and control the export of military and dual-use technology. Through the application of the Export Administration Regulations (EAR), promulgated under the Export Control Reform Act of 2018 (ECRA), the U.S. Department of Commerce, Bureau of Industry and Security (BIS) administers and enforces export controls of "dual-use" commercial items that are not otherwise controlled by the U.S. Department of State, Directorate of Defense Trade Controls (DDTC) under the International Traffic in Arms Regulations.

"Dual-use" is generally defined as those items having civilian applications as well as those having military, terrorism, weapons of mass destruction, or law enforcement related applications. It should be noted that it is a common misperception that ECRA only applies to dual use items. In reality, the EAR cover a broad range of activities which are not limited to dual use items. In addition, the term export includes "the shipment or transmission of the item out of the United States, including the sending or taking of the item out of the United States, in any manner" and "the release or transfer of technology or source code relating to the item to a foreign person in the United States." Accordingly, an "export" can take place even though all of the activity occurred solely within the United States.

Export Control Lists Administered by BIS

The lists described below must be consulted to determine if an export is subject to EAR control and/or if the end user involved in the proposed transaction is one that requires a license to be obtained prior to export.

- The Commerce Control List (CCL) includes items that are subject to control under the EAR. Items that are subject to the EAR but not included on the CCL are designated as EAR99. EAR99 items generally do not require a license to be exported or re-exported but a license may be required if one of the general prohibitions four through ten (described below) apply to the export. As a general matter, EAR99 items consist of low-technology consumer goods.

- The Entity List contains a list of certain foreign persons, including businesses, research institutions, government and private organizations, which are subject to specific license requirements for the export, reexport, and/or transfer (in-country) of specified

items. An EAR99 item that is intended to be exported to a person on the Entity List requires a license even if the EAR99 item could otherwise be exported without a license. The persons and entities on the Entity List have been involved, are involved, or pose a significant risk of becoming involved, in activities that are contrary to the national security or foreign policy interests of the United States.

- The Denied Persons List includes individuals and entities that have been denied export privileges, and any dealings with a party on this list, which would violate the terms of its denial order, are prohibited.

- The Unverified List identifies parties that are ineligible to receive items subject to the EAR by means of a license exception.

- The Military End User List identifies foreign parties that are prohibited from receiving certain items subject to the EAR unless the exporter first secures a license.

EAR General Prohibitions

The EAR includes ten general prohibitions. A violation of these prohibitions and/or a violation of any order, license, or license exception or authorization issued thereunder could result in penalties. Each of the ten general prohibitions should be considered by exporters who deal in products subject to the EAR. The first three general prohibitions are as follows:

- General Prohibition One (Exports and Reexports) – Export and reexport of controlled items to listed countries.

- General Prohibition Two (Parts and Components Reexports) – Reexport and export from abroad of foreign-made items incorporating more than a de minimis amount of controlled for U.S. content.

- General Prohibition Three (Foreign-produced Direct Product Reexports) – Reexport and export from abroad of the foreign-produced direct product of U.S. technology and software.

General prohibitions one through three are product controls that are shaped and limited by the parameters specified on the CCL and the Commerce Country Chart, a listing of countries subject to unique licensing requirements. If a license is required, an application must be submitted unless a license exception applies.

General prohibitions four through ten apply to certain activities that are prohibited without the authorization of BIS and apply to all items subject to the EAR, including items on the CCL and EAR99 items, unless otherwise specified. If any of the general prohibitions four through ten also apply to items subject to general prohibitions one through three, a license will also be required.

- General Prohibition Four – Engaging in actions prohibited by a denial order.

- General Prohibition Five – Export or reexport to prohibited end uses or end users.
- General Prohibition Six – Export or reexport to embargoed destinations.
- General Prohibition Seven – Support of proliferation activities.
- General Prohibition Eight – In-transit shipments and items to be unladen from vessels and aircraft.
- General Prohibition Nine – Violation of any orders, terms, and conditions.
- General Prohibition Ten – Proceeding with transactions with knowledge that a violation has occurred or is about to occur.

EAR Licenses and Due Diligence

BIS licenses may provide authorization to export, reexport or transfer (in-country) products which are otherwise controlled by the restrictions of the EAR. In determining whether a license from BIS is necessary, exporters should make best attempts to self-categorize the products for export and, where necessary, may submit commodity classification requests or requests for an advisory opinion to BIS. Where an exporter determines that a license is necessary to export, reexport, or transfer (in-country) products subject to the EAR, it should submit a formal license application to BIS, often with the assistance of outside counsel.

With regard to EAR due diligence and know your customer (KYC) requirements, certain provisions in the EAR require an exporter to submit an individual validated license application if the exporter “knows” that an export that is otherwise exempt from the validated licensing requirements is for end-uses involving nuclear, chemical, and biological weapons, or related missile

delivery systems, in named destinations listed in the EAR.

EAR compliance requires companies to maintain robust export compliance programs. The EAR includes a list of "red flags" that should be taken into account in know your customer analyses. These include, for example:

- Orders which are inconsistent with the needs of the purchaser;
- A customer declining installation and testing when included in the sales price or normally requested; or
- Requests for equipment configurations that are incompatible with the stated destination (e.g., 120 volts in a country which uses 220 volts).

As with OFAC, BIS encourages the submission of voluntary self-disclosures by parties who believe they may have violated the EAR and such disclosure often are a significant mitigating factor in determining what penalties, if any, will be sought.

Potential Penalties for Non-Compliance with EAR

Violations of the EAR, or any license issued thereunder, may carry significant penalties, including civil fines, the possibility of imprisonment for up to 20 years for intentional and willful violations, and/or the revocation of licenses and denial of eligibility to export and re-export, depending on the nature of the violation.

Civil penalties for violations of the EAR may include, but shall not exceed: (1) $300,000, or (2) an amount twice the value of the transaction that is the basis of the violation with respect to which the penalty was imposed, whichever is greater. In addition to these civil penalties, the Department of Commerce may also revoke a license issued under the EAR or prohibit a person/entity's ability to export, reexport, or transfer (in-country) any item(s) controlled thereunder.

An individual or company may be criminally liable for willful violations, willful attempts at violations, and willful conspiracies to violate the ECRA, as well as aiding and abetting the commission of such violations. Criminal penalties may include, but shall not exceed: (1) $1,000,000 per violation, (2) 20 years' imprisonment, or (3) both (1) and (2). In addition to these criminal penalties, the Secretary of Commerce may deny eligibility to export, reexport, or transfer(in-country) any item, whether or not subject to controls under subchapter one of the ECRA, for a period of up to ten years beginning on the date of conviction of a criminal violation of any regulation, license or order issued under subchapter one of the ECRA, as well as other additional types of violations provided for in

the regulations. The Secretary of Commerce may also revoke any license or other authorization to export, reexport, or transfer items that was issued under subchapter one of the ECRA and in which such person has an interest at the time of conviction.

Additionally, eligibility for export administered by the U.S. Department of State may be restricted and the right to contract with the U.S. Department of Defense and other agencies may be suspended due to conduct that violates the ECRA or the EAR, or any order, license, or authorization issued thereunder.

Investigations and Recent Enforcement Activity

Within BIS, the Office of Export Enforcement investigates criminal and administrative violations of the dual-use export regime, conducting domestic investigations, and working with U.S. Immigration and Customs Enforcement at the U.S. Department of Homeland Security to conduct international investigations. Civil violations are referred to the Office of Chief Counsel for BIS and criminal violations are referred to the U.S. Department of Justice.

In its Export Enforcement: 2023 Year in Review, BIS reported examples of recent enforcement actions under the ECRA as follows:

- *United States v. Hans De Deetere:* Based on indictments unsealed in December 2023, BIS, working in coordination with the DOJ, charged a Belgian national for a scheme to export military-grade technology, including accelerometers and missile components, to China and Russia. BIS' Disruptive Technology Task Force determined that, between March 2016 and February 2018, Hans De Deetere worked with co-Defendants to illegally smuggle from the United States export-controlled programmable gate array (FGPA) circuits to Russia and short-wave infrared surveillance (SWIR) camera to the People's Republic of China.

- *United States v. Seagate:* In April 2023, BIS announced the largest standalone administrative penalty in its history, a $300 million penalty against Seagate and Seagate International Headquarters Pte. Ltd. of Singapore (collectively, Seagate) related to its shipment

of millions of hard disk drives (HDDs) to Huawei Technologies Co. Ltd. (Huawei). In 2020, BIS imposed controls over certain foreign-produced items related to Huawei. Despite this action, BIS determined that, between August 2020 and September 2021, Seagate ordered or cause the reexport of approximately 7 million UDDs to Huawei entities listed on the BIS Entity List or where such entities were a party to a transaction without authorization from BIS.

INTERNATIONAL TRAFFIC IN ARMS REGULATIONS (ITAR): THE BASICS

While the EAR controls the export, reexport, and transfer of commercial items and certain dual-use items, the International Traffic in Arms Regulations (ITAR) is the cornerstone of U.S. military/munitions export control law. As with the EAR, ITAR defines the term "export" broadly. The term applies to exports of tangible (e.g., defense articles) and intangible (e.g., defense services, technology or information) items out of the United States. It also includes the "release" or passing of information or technology to foreign persons even if in the United States.

The ITAR implement the Arms Export Control Act (AECA) and controls the manufacture, export, and temporary import of defense articles (including technical data), the furnishing of defense services, and brokering activities involving items described on the United States Munitions List (USML). The Department of State's Directorate of Defense Trade Controls (DDTC), an agency within the Department of State's Bureau of Political-Military Affairs, administers and enforces the ITAR.

Categories of Items Controlled under ITAR

The USML controls many items that may be similar to those commercial items controlled by the EAR. When conducting jurisdiction and classification analyses, it is important to recall that a difference in form, fit, function, performance, and testing or certification procedure can be determinative of whether that product or service is controlled by the ITAR, EAR or neither. If both the USML and the CCL appear to describe an item, the exporter must presume that the item is controlled by the ITAR.

The USML designates particular types of equipment as "defense articles" and divides ITAR-controlled items into 21 specific categories. If an item appears to be described in multiple USML entries, it should be classified in the more specific USML entry. The specific categories under the ITAR are generally segregated into three "types" of exports:

- *Defense articles* are items and related technical data that are specifically designed, developed, configured, adapted, or modified for a controlled use listed on the USML.
- *Technical data* means any information for the design, development, assembly, production, operation, repair, testing, maintenance, or modification of a defense article.
- *Defense services* include assisting foreign persons in the design, development, manufacture, assembly, repair, maintenance, modification, or use of defense articles, as well as providing technical data, whether in the United States or abroad. It also includes military training of foreign armed forces through furnishing military advice, courses and correspondence, and training aids, whether in the U.S. or abroad.

ITAR Registration

Persons and entities in the United States that engage in ITAR-regulated activities must register with DDTC before exporting defense articles and/or defense services and pay a yearly fee whether or not the

person seeks to export during that specific year. Registration with DDTC is a means to provide the U.S. Government with necessary information on who is involved in certain ITAR-controlled activities and does not confer any export or temporary import rights or privileges. Registration is generally a precondition for the issuance of any license or other approval and use of certain exemptions.

Authorization to Export

Once ITAR registration is complete, any person or company who intends to export or temporarily import a defense article, defense service, or technical data must apply for authorization from DDTC, unless an exemption applies. Under the ITAR, the two primary types of authorizations include:

- Licenses: These are typically used for shipments of hardware, but may also be used for shipments of technical data and employment on non-U.S. persons.

- Agreements: Used when providing a "defense service," though they can also authorize the shipment of related technical data and hardware, ITAR agreements are essentially a State Department agreed contract between the exporter and the foreign licensee which outlines the scope of the exported defense services, technical data, or hardware, and include ITAR required control language. There are three general categories of ITAR agreements:

  - Technical Assistance Agreements (TAAs): A TAA is an agreement between a company or individual in the U.S. and a foreign entity that allows for the provision of defense services and/or transfer of technical data or assistance, subject to the restrictions contained in the agreement.

  - Manufacturing License Agreements (MLAs): An MLA is an agreement between a company or individual in the U.S. and a foreign entity that allows for the manufacture of items subject to the ITAR in a foreign country.

  - Warehouse and Distribution Agreements (WDAs): A WDA is an agreement between a company or individual in the U.S. and a foreign entity that allows for a warehouse or distribution center for an ITAR-controlled item to be located in a foreign country.

DDTC reviews all requests to export, reexport, retransfer, or temporarily import defense articles or defense services or to engage in brokering activities on a case-by-case basis. There is no presumption of approval for submissions and DDTC may disapprove license or agreement applications that are not in furtherance of the national security or foreign policy of the U.S.

Finally, the ITAR generally prohibit U.S. persons and/or companies from obtaining a license to export or temporarily import defense articles or services from certain countries, including North Korea, Iran and Syria. Should a company know of an ITAR-controlled transaction involving a country subject to an arms embargo, then it has a duty to notify the DDTC's Compliance Office immediately.

Commodity Jurisdiction Requests

While DDTC has jurisdiction over deciding whether an item is ITAR- or EAR-controlled, it encourages

exporters to self-classify their products and services. If doubt exists as to the classification of an item, entities may submit a written commodity jurisdiction (CJ) request to DDTC. Upon receiving such a request, DDTC will provide guidance as to whether a particular product or service is subject to the ITAR or EAR.

Potential Penalties for Non-Compliance with ITAR

DDTC is responsible for civil enforcement of the ITAR and the U.S. Department of Justice handles criminal enforcement matters. Similar to sanctions administered by OFAC, the ITAR is a strict liability regime. U.S. individuals and entities may be subject to civil liability regardless of whether they intended to violate the ITAR. Meanwhile, criminal liability generally requires a person to willfully (1) violate any provision of the AECA or the ITAR; or (2) make or omit an untrue statement of a material fact in a registration, license application, or required report. Civil penalties may be imposed in conjunction with criminal penalties. DDTC's options to address civil ITAR violations include: (1) financial penalties up to $1,200,000 per violation; (2) suspension of export privileges; or (3) debarment of up to three-years from ITAR-regulated defense trade.

For criminal violations, a person may be subject to: (1) a maximum fine of $1,000,000 for each violation, (2) up to 20 years' imprisonment, or (3) both (1) and (2).

Additionally, DDTC maintains a list of persons who have been statutorily and administratively debarred. Persons convicted of violating, or conspiracy to violate, the AECA are subject to statutory debarment. These persons are prohibited from participating directly or indirectly in the export of defense articles and services. A statutory debarment remains in effect unless the debarred person's application for reinstatement of export privileges is granted by DDTC. On the other hand, DDTC may impose administrative debarment for violations of either the AECA or ITAR upon resolution of enforcement proceedings. It is the exporter's responsibility to verify all parties to a transaction are eligible. Debarment lists are published in the Federal Register and on the DDTC website.

As with OFAC and BIS, DDTC encourages voluntary self-disclosure of apparent ITAR violations. DDTC considers voluntary disclosures to be a mitigating factor when determining the appropriate administrative penalties, if any, in response to a particular case. Such a voluntary disclosure must occur prior to, or simultaneous with, the discovery by the U.S. Department of State or another government agency of the apparent violation or a substantially similar apparent violation.

Recent Enforcement Actions

- *United States v. 3D Systems Corporation:* On February 27, 2023, DDTC announced the conclusion of a $20,000,000 administrative settlement with 3D Systems Corporation to resolve alleged violations of the AECA and ITAR. In summary, DDTC found that 3D Systems had, from 2012 to 2018, provided unauthorized exports of technical data to Germany, China, Taiwan, and foreign-person employees. Additionally, 3D Systems failed to maintain adequate ITAR records. In addition to the administrative penalty, 3D Systems was required to engage and external Special Compliance Office, which would be charged with conducting external audits of its compliance program and implementing additional compliance measures.

- *United States v. Baier:* On September 7, 2021, former U.S. Intelligence Community and military personnel entered into a deferred prosecution agreement (DPA) to resolve allegations that the defendants violated the ITAR by providing defense services — using their knowledge of offensive cyber capabilities — to a United Arab Emirates (UAE)-based company carrying out hacking operations on behalf of the UAE government, absent a

DDTC license. The alleged defense services included support, direction, and supervision in the creation of sophisticated "zero-click" computer hacking and intelligence gathering systems. Employees of the UAE-based company were alleged to then leverage the zero-click exploits to illegally obtain and use access credentials for online accounts issued by U.S. companies, and to obtain unauthorized access to computers around the world, including in the United States. The DPA required the defendants to pay over $1.6 million and imposed a lifetime ban on holding U.S. security clearances and government employment. This marked the first time the U.S. Department of Justice charged hacking as a violation of the ITAR.

- *In the Matter of Airbus SE:* On January 29, 2020, Airbus SE (Airbus), a multinational aerospace corporation, agreed to settle 75 charges in connection with alleged violations of the AECA and the ITAR by its subsidiaries. The charges included providing false statements on authorization requests, failure to provide accurate and complete reporting on political contributions, commissions, or fees that it paid in connection with sales, failure to maintain records involving ITAR-controlled transactions, and the unauthorized reexport and retransfer of defense articles. For example, Airbus sought authorizations for the export, reexport, or retransfer of defense articles or provision of defense services without providing accurate statements for sales to or for the use of the armed forces of Colombia, Egypt, Ghana, Indonesia, Jordan, Kazakhstan, Mexico, Poland, and Vietnam. These transactions required DDTC approval because Airbus incorporated ITAR-controlled defense articles into the aircrafts at issue. Despite submitting voluntary self-disclosures, Airbus was found to have significant deficiencies within its compliance program and poor recordkeeping. The DDTC imposed a $10 million penalty against Airbus.

BUCHANAN'S EXPERIENCE WITH ECONOMIC SANCTIONS AND EXPORT CONTROLS

For individuals and entities doing business in this new era of expanded sanctions and controls administered by the OFAC, having a team of experienced lawyers is a necessity to fully comply with the nuances of the various laws and outlined in this handbook. Buchanan Ingersoll and Rooney's team of National Security attorneys are intimately familiar with these regimes and remain abreast of the latest developments and DOJ enforcement actions. Our attorneys routinely counsel and advise clients in relation to OFAC, BIS, and ITAR licenses, requests for advisory opinions, record keeping requirements, audits, compliance training, voluntary disclosures, and potential enforcement actions.

Buchanan's International Trade & National Security practice group members have fostered excellent working relationships with key federal regulatory bodies, and routinely represent clients on issues before OFAC, BIS and DDTC and stand ready to guide individuals and entities through these continuing evolving matters.

Daniel B. Pickard

Chair, International Trade & National Security Practice Group

Email: daniel.pickard@bipc.com
Phone: (202) 452-7936

In his specialty practice, Dan Pickard brings more than 20 years of experience providing guidance pertaining to foreign policy and national security matters such as U.S. economic sanctions and export controls, including the International Traffic in Arms Regulations (ITAR), anti-boycott measures, and the Foreign Corrupt Practices Act (FCPA). Dan provides comprehensive international trade law compliance guidance, including to U.S. and international clients that provide goods and services that may be regulated due to national security reasons. He has extensive experience in matters related to trade remedy investigations, including antidumping, countervailing duty, and safeguard cases, which provide relief to U.S. producers who have been injured as a result of import competition. Dan develops customized and specialized corporate compliance programs related to the NISPOM, FCPA, ITAR, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), the Foreign Agents Registration Act (FARA), and mitigating Foreign Ownership, Control, or Influence (FOCI) issues.