Arnold & Porter

Compliance as a Catalyst: Turning Export Control into Competitive Edge

Authors: Trevor Schmitt, Bell Johnson, Michael Hochberg*

ACKNOWLEDGMENTS

The authors would like to thank Matt Russell for his extensive help with editing and organizing this project. Michael Hochberg would like to thank Rodger Baker for his advice and Christine Clay for all of her help and support, which made this project possible.

DISCLAIMER

This document and the information contained herein do not constitute, nor should they be relied upon as, legal advice. Specific terms and provisions of your export controls compliance policies and procedures should be based on your specific circumstances and tailored to meet the specific legal and commercial requirements of your business operations. Additional policies, procedures, and processes may be required for you to meet applicable legal requirements. You are responsible for ensuring that all necessary compliance requirements are met in connection with your business activities. You should consult with an attorney licensed to practice in your jurisdiction before using or relying on the information contained herein.

* Not admitted to the practice of law

Introduction

Export controls are an area of the law that presents both enormous challenges and the opportunity for significant differentiated advantage, particularly for startup companies. As the post-World War II liberal-democratic order has started to break down, the United States and its allies have applied an ever more complex series of laws, policies, and regulations to the movement of both tangible and intangible goods. These laws apply not only to the physical or electronic export of objects, but to sharing information even within the United States with non-U.S. persons. The relevant laws are byzantine, complex, arcane, and frequently incomprehensible to ordinary engineers and executives. The penalties for failing to properly comply with these laws range from fines to jail time; these penalties are generally much more severe in the United States than in allied states.

For example, the U.S. Department of the Commerce's Bureau of Industry and Security (BIS) entered into a US$300 million settlement in April 2023 with Seagate Technology LLC ("Seagate") to resolve alleged export control violations related to shipments of hard disk drives (HDDs) to Huawei Technologies Co. Ltd. ("Huawei"). It was Seagate's belief that its HDDs were not subject to U.S. export control restrictions because they were produced outside of the United States. However, Seagate's HDDs were produced with equipment made with U.S.-origin-technology, rendering the HDDs subject to U.S. export controls under the Foreign-Direct Product Rule (FDPR).

On June 24, 2024, BIS announced that it had reached a settlement with, and was issuing an administrative penalty on, Indiana University-Bloomington (IU) as part of a larger settlement related to the university's violation of U.S. export controls. According to BIS, IU exported shipments of varying genetically modified fruit flies to 30 different research institutions in 16 destinations without first obtaining a required U.S. export control license.

More recently, RTX Corporation ("RTX") entered into a US$200 million settlement agreement on August 30, 2024 with the U.S. Department of State's Directorate of Defense Trade Controls (DDTC) for various violations of U.S. export controls. Among other things, RTX failed to appropriately classify its products, resulting in U.S. export violations when such products were exported to RTX affiliates in France and Germany — both close allies of the United States. RTX employees also carried cell phones and laptops containing U.S. export-controlled information to unauthorized locations during personal travel without first seeking the required U.S.-governmental approval. Such actions have previously resulted in employees serving jail time. For example, an electrical engineer at Raytheon Missiles and Defense (RMD) took his laptop — which contained export-controlled information — abroad, despite RMD's explicit prohibition on doing so. The employee was sentenced to 38 months in prison for knowingly exporting controlled weapons technology plans out of the United States to China.

With increasing enforcement, export controls have moved from being an obscure corner of the legal world to a source of both danger and differentiation for companies of all sizes. It remains common for small-company founders and executives to be ignorant of export law, despite the increased danger of enforcement action over the past few years. But ignoring these regulations is a mistake: Companies that set themselves up to be compliant by default with these

regulations will avoid enormous problems, including legal consequences, operational complexity, and potentially failed M/A and exits. Having a working knowledge of these regulations will allow executives to design their organizations and procedures so that the number of exceptions and amount of overhead are reduced to the bare minimum, and will allow them to manage legal and operational risks. Companies that do this successfully will generate, in some cases, decisive operational advantages over the ones that treat compliance as an afterthought.

Our goal here is to provide a relatively simple explanation of how these laws work, aimed primarily at U.S. startup executives, so that they can design their businesses from a position of knowledge rather than ignorance. In the final section, we provide a practical framework for keeping the operational implementation of these rules as simple as possible, so that technology startups can focus on their core mission.

Origins of U.S. Export Controls and the Current Regimes

Export controls in the United States have a long history — dating back to the early days of the republic — but the modern era of export controls began during World War II. In 1940, Congress authorized the President to control the export of military equipment and munitions. This authority was later expanded to include civilian goods. As Cold War tensions increased in the late 1940s, export controls began to be seen as a valuable foreign policy and national security tool, and with the enactment of the Export Control Act (ECA) in 1949, the United States established a four-pronged strategy that underlies the modern regime: This strategy involved using export controls to (i) protect the domestic economy, (ii) further U.S. foreign policy, (iii) influence or otherwise coerce foreign state actions, and (iv) safeguard national security. There is considerable debate in the policy community about the efficacy of export controls as a tool for coercion.

Over the years, this system has evolved with significant new legislative and regulatory frameworks. The current U.S. export control regime relies primarily on the Export Control Reform Act (ECRA), which provides permanent statutory authority for dual-use export controls (i.e., goods and technologies that have both commercial and military applications), the Arms Export Control Act (AECA) for military items and related services, and nuclear-specific legislation for nuclear materials and technology, the International Emergency Economic Powers Act (IEEPA). For economic sanctions, the United States also relies on various regime-specific legislation, such as the Trading with the Enemy Act, the IEEPA, the Iran Sanctions Act, and the United Nations Participation Act. This system is administered by multiple agencies, including the Departments of Commerce, State, and Treasury, with enforcement support from the Departments of Homeland Security and Justice. These separate agencies often have divergent priorities and conflicting interpretations of the relevant laws and regulations. For those who are unfamiliar with the byzantine workings of the federal bureaucracy, such conflicting interpretations are often surprising and frustrating.

These regimes are implemented through the following regulations:

- International Traffic in Arms Regulations (ITAR), 22 C.F.R. 120-130 administered by the U.S. Department of State, DDTC
- Export Administration Regulations (EAR), 15 C.F.R. 730-780 administered by BIS
- Office of Foreign Assets Control (OFAC), 31 C.F.R. 500-599
- Nuclear Regulatory Commission (NRC), 10 C.F.R. 110

Export controls have undergone significant changes over the decades, driven by geopolitical shifts, technological advances, and changes in U.S. policy. A recent example of this new trend

was the deployment of nearly comprehensive export controls on Russia following its further invasion into Ukraine in February 2022.[1] The United States has also used export controls in recent times to respond to human rights abuses and other foreign policy concerns. It remains an open question as to how effective export controls and sanctions restrictions are in terms of influencing foreign state actions; yet restrictive actions undertaken by the United States should not impede other domestic priorities or objectives of the country.

Despite all the effort and attention paid to restricting Iranian and Russian oil and gas exports, the total volumes of these products being shipped overseas have not been significantly impacted. The flows of trade have shifted, with much of the production capacity of Russian and Iranian hydrocarbons making their way to China, through the use of a "shadow fleet" of tankers. But Russian and Iranian revenues from these sources do not appear to have been dramatically impacted; sanctions have been more of an inconvenience than a genuine barrier.

New trends also include a heightened focus on controlling exports to strategic competitors — particularly China — by tightening restrictions on semiconductor chips and related equipment, as well as increased attention on how to monitor and control emerging technologies like Artificial Intelligence (AI) and quantum computing. These measures add to new restrictions on technology transfers to Chinese firms involved in military and surveillance activities, addressing the risks posed by emerging and foundational technologies.

Enforcement of Export Control Violations

The U.S. government generally imposes various standards of liability under export controls and sanctions law, including, in many instances, a strict liability standard — which means that individuals and companies are liable for certain violations even if they do not intend to break the law or know that their actions could violate the restrictions. Violations of the EAR and ITAR can include up to 20 years of imprisonment for criminal penalties and up to US$1 million in fines per violation. Administrative penalties of up to US$300,000 per violation (subject to inflationary changes) or twice the value of the transaction — whichever is greater — can also be imposed. Individuals can also be stripped of their export privileges.

That being said, the regulations include provisions for individuals and entities that voluntarily disclose suspected violations to the appropriate agencies. By notifying the U.S. government of potential violations, the disclosing party may receive a 50% reduction in any monetary penalty the U.S. government may seek to impose. Substantial cooperation with the U.S. government can result in an even greater mitigating credit. When ascertaining the kind of penalty to impose, the U.S. government takes into account several aggravating and mitigating factors:

Aggravating Factors	Mitigating Factors
Willful or reckless violation of the law	Remedial response
Awareness of conduct at issue	Exceptional cooperation with enforcement proceedings
Harm to regulatory program objectives	Likelihood of license approval, if previously sought

The U.S. government will also consider whether there are related violations, multiple unrelated violations, or previous enforcement actions taken against the relevant party. In addition, the future compliance and deterrent effect an administrative enforcement action may have on

[1] The ongoing Russo-Ukrainian War began in February 2014 following Russia's annexation of Crimea from Ukraine. *See*, PAUL K. KERR & CHRISTOPHER A. CASEY, CONG. RSCH. SERV., R46814, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL REFORM ACT OF 2018 (2021).

promoting future compliance within the industry is another factor weighed by the U.S. government.

In the wake of Russia's further invasion of Ukraine in 2022, growing competition with China, and other global challenges, the U.S. government has increasingly prioritized export controls enforcement by allocating additional resources to enforcing export controls. For example, the Department of Justice's National Security Division hired 25 new prosecutors in 2023 to specifically investigate and prosecute export controls, sanctions, and similar economic crimes. The U.S. government has also strengthened export enforcement by increasing interagency coordination, including the creation of new task forces, such as the Disruptive Technology Strike Force (DTSF).[2] Recent enforcement actions reflect a trend of strict enforcement and increasingly high penalties, particularly where the conduct was deceptive.

With an increased focus on export controls enforcement, individuals and companies can better protect themselves against adverse enforcement actions by developing robust compliance programs, as well as conducting and preserving due diligence efforts. Should an apparent export control or sanctions violation arise, individuals and companies may also reduce exposure by filing voluntary disclosures and taking mitigating and remediating steps.

What Does This Mean for You?

Different companies deal with these laws in different ways. Designing an effective compliance program depends closely on the actual operations of the company: A firm that makes only one physical product, sells it domestically, hires infrequently, and uses little high-technology software or equipment needs different internal procedures than one that operates internationally, works with sensitive technology, and is expanding rapidly.

In general, there are five common sources of compliance complexity with regard to export control:

1. Products: Nearly all commodities, software, and non-"published" technology is subject to U.S. export controls. Depending on the relevant jurisdiction and classification of the item, an export control license authorization or use of a license exception may be required prior to exporting, reexporting, or transferring (in-country) an item made in the United States to any location worldwide. These controls apply not only when the item is initially exported from the United States, but also when the item is sent between third countries. Therefore, accurate jurisdiction and classification determinations are essential for any organization that engages in international business.
2. Customers: Outside of narrow circumstances, shipping a product to an overseas customer is an export and thus is subject to U.S. export controls. But consideration should also be given to selling a product to a customer within the United States, as that customer may be a "prohibited party" (i.e., individuals, corporations, research institutions, and government organizations deemed to pose a risk to U.S. national security, foreign, and economic policy).[3] Selling to a customer who has expressed an intention to resell the product should also warrant further review, as it may indicate

[2] The interagency DTSF was launched in 2023 to bring criminal enforcement actions against actors who circumvent export controls on Russia as well as on China and Iran.

[3] The U.S. government maintains a series of federal laws and regulatory regimes designed to prohibit certain activities with specific individuals or entities. These "Restricted Party Lists" comprise names, aliases, and addresses of individuals and entities and include but are not limited to the following: (i) Specially Designated Nationals and Blocked Persons List, (ii) Entity List, (iii) Denied Persons List, (iv) Military End User List, (v) Debarred List, and (vi) Communist Chinese Military Companies List.

potential evasion tactics. It is necessary to understand the export status of your products and, before selling to customers in a given jurisdiction, to determine what authorizations, letters of assurance, or other procedures are required. The pre-sales and support phases are highly complex. Electronic transmission of confidential data, software, or design files constitutes an export event and must be treated accordingly, even if it occurs wholly within the United States. Therefore, careful consideration should be given to the location and the nationality of the individual receiving the electronic transmission.

3. Vendors: As with customers, vendor interactions are often a source of complexity. Vendors should be reviewed carefully to ensure that no prohibited parties are present. For any items they supply, vendors should disclose the applicable export control jurisdiction and classification. This can become increasingly more complicated when you furnish vendors with design data, specifications, software, or training. In short, export control restrictions apply to all stages of a supply chain and due diligence is needed for each flow.
4. Investors: The Committee on Foreign Investment in the United States (CFIUS or the "Committee") maintains jurisdiction to review certain investments in U.S. businesses and real estate. If, following review of a transaction, CFIUS determines that the transaction involves national security concerns, the Committee may seek to mitigate those concerns through a national security agreement, or recommend the President block or otherwise unwind the transactions. These reviews apply to full controlling transactions as well as certain partial investments by foreign persons, and may be voluntary — i.e., once CFIUS reviews a voluntarily submitted filing regarding the transaction — or mandatory. Parties that fail to submit a mandatory filing face stiff penalties and other consequences.
5. Hires: Hiring, whether for full-time employees or contractors, is fraught with export complexity and additional steps may need to be taken if non-U.S. persons are hired. This is because, under the EAR, an export can occur through the release of "technology" or source code to a foreign person located in the United States, as such a release is usually deemed to be an export to the foreign person's most recent country of citizenship or permanent residency. In other words, releasing technology to an Iranian citizen who does not qualify as a U.S. person,[4] who is working for a company or university in the United States, may constitute an export to Iran. However, a disclosure to the same person who had become a permanent resident of Canada before residing in the United States would constitute a deemed export to Canada, not Iran, under the EAR (the ITAR is more restrictive and considers a person's current *and* past citizenships as well as country of birth). As part of the hiring process, it is desirable to determine the export control status of each prospective employee as soon as possible. Hiring a staff member or contractor who will need a license is a time-consuming and risky endeavor, especially for a small firm, as such a hire may be idle until the license is obtained. The licensing process can take many months or even years, cost tens of thousands of dollars in legal fees, and the license may, in fact, never be granted. Further, the U.S. Department of Justice regularly initiates anti-discrimination enforcement actions against businesses that incorrectly interpret U.S. export control licensing requirements.

In all of these cases, it is important to implement both legal and operational protections. Legal protections in the form of language in contracts, subscription agreements, purchase orders, etc.

[4] A U.S. person is a natural person who is a lawful permanent resident as defined in 8 U.S.C. § 1101(a)(20) or who is a protected individual as defined by 8 U.S.C. § 1324b(a)(3). It also means any corporation, business association, partnership, society, trust, or any other entity, organization or group that is incorporated to do business in the United States. It also includes any governmental (federal, state, or local) entity.

make it clear that the counterparty is aware of export control restrictions and will take responsibility for compliance with the relevant laws, regardless of where they are based. Operational checks are required in order to ensure that, when there is an export event, it is handled properly and that data or material is not placed in the hands of unauthorized parties. Certain recordkeeping requirements are stipulated under the regulations. Furthermore, evidence of a good- faith effort at compliance is a key mitigating factor in any investigation of export violations.

Simplicity is key in developing an export control process and compliance program for startup companies. Experience shows that technical personnel are often resistant to learning any of the details of what they regard as encumbrances to their work. As a result, being able to issue clear guidance is essential.

For instance, at an organization where all employees are U.S. persons, a simple “whitelist” item might state: “Any technical data that we possess may be shared, using company servers, with any employee; the employee list is linked below.” A similar “blacklist” item might read: “Before sharing any technical information with anyone who is not an employee, seek permission from the Export Control Officer (ECO) or a VP” or “Before shipping any equipment overseas for any reason, seek permission from the ECO or a VP.” These kinds of simple rules tend to eliminate the improvisation that often creates accidental export violations. By creating simple guidelines that refer employees to experts, the burden of training the entire company to comprehend the nuances of U.S. export control restrictions is reduced. Such training programs rarely succeed beyond making employees aware that exports of various sorts need specialist help, since export control is complex. That being said, general awareness of export controls should be provided to all employees, with more tailored training for individuals directly engaged in monitoring and ensuring compliance.

While these regimes are often strict liability, the U.S. government does take into account good faith efforts to comply with these restrictions. A company’s lack of a — or an inadequate — export compliance program can be an aggravating factor in enforcement actions, potentially leading to increased penalties for violations. Conversely, a company’s investment of time and resources into developing a compliance program may help reduce potential fines. Ultimately, the U.S. government wants to ensure that industry is aware of its obligations under export controls and sanctions restrictions and is applying a risk-based approach to its operations.

Overview of U.S. Export Controls

This document is intended to provide a high-level overview of the framework of legal regimes a startup may encounter with respect to U.S. export control and sanctions regulations. As discussed above, you should engage outside counsel prior to undertaking any of the activities discussed below that may implicate U.S. export control and sanctions.

I. EAR

The EAR, administered by the BIS, regulates the export of commercial and dual-use goods and technology to any foreign designation or foreign person — whether located in the United States or abroad — and requires U.S. entities to comply with licensing, recordkeeping, and reporting requirements.

Under the regulations, the term "item" refers to commodities, software, and technology not otherwise subject to a more restrictive export control regime. Each of the terms—commodities, software, and technology—has its own definition under the EAR.[5] Notably, technology may be in any tangible or *intangible* form, such as written or oral communications.

The following items are subject to the EAR:

1. All items in the United States, including in a U.S. Foreign Trade Zone or moving in transit through the United States from one foreign country to another, including where U.S.-based facilities are used to store or transmit software to a party outside of the United States (e.g., if a U.S. data center is used, everything that passes through the U.S. data center is subject to the EAR);
2. All U.S.-origin items, wherever located;
3. Foreign-made commodities that incorporate controlled U.S.-origin commodities, foreign-made commodities that are "bundled" with controlled U.S.-origin software, foreign-made software that is commingled with controlled U.S.-origin software, and foreign-made technology that is commingled with controlled U.S.-origin technology:
    i) In any quantity, for certain items, and
    ii) In quantities exceeding the de minimis levels, for most other items;
4. Certain foreign-made direct products of U.S.-origin technology or software. The term "direct product" means the immediate product (including processes and services) produced directly by the use of technology or software; and

[5] 15 C.F.R. Part 772.

5. Certain commodities produced by any plant or major component of a plant located outside of the United States that is a direct product of U.S.-origin technology or software.[6]

There is nuance to the application of these standards, but generally the EAR covers everything produced in the United States, even a pen or a pencil. What it does not cover are all goods, software, or technology produced outside of the United States, even where U.S. content is incorporated into the goods, software, or technology, or U.S. software or technology is used to make the goods. Rather, non-U.S. producers and developers must assess what materials and components (in the case of goods) or U.S. code or technical information (in the case of software or technology) are incorporated into their non-U.S. produced items. Separately, non-U.S. producers must consider whether and what U.S. software or technology was used in the production or development of the non-U.S. item (but not incorporated into it). This analysis informs what items are subject to the EAR and is nuanced.

For example, a simple printer produced in the United States is subject to the EAR at a low control level (but still restricted for parties like Huawei on the Entity List). That same printer produced using a U.S. blueprint, but in China, would not be subject to the EAR. If, however, an expensive control unit made in the United States is incorporated into the non-U.S. produced printer, the printer could nonetheless become controlled by virtue of the value of that control unit as a percentage of the entire printer. Change the scenario slightly so that instead of a simple printer, the object in question is a high-precision semiconductor fabrication machine. Now, even if the machine is produced outside of the United States — and even if no material or components incorporated into the machine are U.S. origin — if the machine is based on controlled U.S.-origin blueprints, the machine itself could be subject to the EAR (depending on precisely at what level the blueprints are controlled).

Not all information contained in documents is determined to be subject to U.S. export control restrictions if it is in the "public domain."[7] This includes information which is published and is generally accessible or available to the public:[8]

- Through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, generally accessible to the public, in the United States;
- Through patents available at any patent office;
- At libraries open to the public or from which the public can obtain documents, or at newsstands, bookstores, etc.;
- Public dissemination (i.e., unlimited distribution) in any form (e.g., not necessarily in published form), including posting on the internet on sites available to the public;[9] or

[6] 15 C.F.R. § 734.3(a).

[7] 15 C.F.R. § 734.3(b); 22 C.F.R. § 120.34.

[8] 15 C.F.R. § 734.7.

[9] Public internet location of open source encryption software must be sent to the U.S. government before it is considered "published." Under 15 C.F.R. § 742.15, publicly available encryption source code is not subject to EAR controls if the developer notifies the U.S. government "via email of the Internet location (e.g., URL or internet address) of the publicly available encryption source code . . . or provide each of them a copy of the publicly available encryption source code. . . . In all instances, submit the notification or copy to crypt@bis.doc.gov and to enc@nsa.gov."). Usually, the original developer notifies the U.S. government of the software to release it from control, but any party can send the government the Internet location where the software is available to ensure it is treated as "open source" under the EAR.

- Through Fundamental Research (i.e., research in science and engineering at accredited institutions of higher learning in the United States, the results of which ordinarily are published and shared broadly within the research community, and for which the researchers have not accepted restrictions for proprietary or national security reasons).[10]

Importantly, while the Fundamental Research Exception (FRE) is broadly defined, it does not apply when restrictions are placed on the outcome of the research or on the methods used. Proprietary research; industrial development, design, production, and product utilization whose results are restricted; and government-funded research that specifically restricts outcomes for national security reasons are not considered fundamental research.[11] In general, if the results of the research are covered by an non-disclosure agreement, and if any party has a right to veto or greatly delay publication, the FRE may not be applicable. Even if the basic project is determined to meet the FRE, certain aspects of the project may still be subject to U.S. export control restrictions, such as: shipping tangible items, foreign national access, work conducted outside the United States, or use of types of specific software (e.g., encryption). A checklist to help determine whether the FRE applies can be found in Annex 1.

While the EAR is generally flexible, if an item is subject to the EAR, then any transfer of the item to another party (other than a U.S. person),[12] even between two non-U.S. parties located in the same country, must be checked against the regulations before transfer. Certain restrictions may prohibit its transfer, and different licensing requirements may apply. Items can be transferred in one of three ways: export, reexport, and transfer (in-country).

An export is generally defined as:

- An actual shipment or transmission out of the United States, including the sending or taking of an item out of the United States, in any manner;
- Releasing or otherwise transferring technology to a foreign person in the United States (a “deemed export”); or
- Transferring by a person in the United States of registration, control, or ownership of certain spacecraft.[13]

Meanwhile, a reexport occurs when there is:

- An actual shipment or transmission of an item subject to the EAR from one foreign country to another foreign country, including the sending or taking of an item to or from such countries in any manner;
- Releasing or otherwise transferring technology to a foreign person of a country other than the foreign country where the release or transfer takes place (a deemed reexport); or
- Transferring by a person outside of the United States of registration, control, or ownership of certain spacecraft.[14]

---

[10] 15 C.F.R. § 734.8(a); 22 C.F.R. § 120.34(a)(8).

[11] *Id.*

[12] Failure to adhere to U.S.-Person-related requirements may result in discrimination-based enforcement actions.

[13] 15 C.F.R. § 734.13.

[14] 15 C.F.R. § 734.14.

Finally, a transfer (in-country) is defined as a change in end use or end user of an item within the same foreign country.[15]

Generally, there are three kinds of transfer controls: country-level, end user, and end use.

First, transferors must review the Commerce Control List (CCL), which contains Export Control Classification Numbers (ECCNs). ECCNs list specific items and detail the level at which the listed items subject to the EAR are controlled.[16] If an item is not listed on the CCL, but is subject to the EAR, then it is classified "EAR99."

Non-experts should be extremely cautious in reading the CCL and attempting to self-determine the ECCNs related to their work: Plain-language interpretations of the CCL will *very often* yield incorrect results. The use of language in the CCL is not identical to colloquial English, and there is an extensive body of bureaucratic rulings and interpretations for how to read the CCL. Consulting an expert in determining an ECCN is generally advisable. Both maximalist and minimalist approaches in terms of the conservatism of the classification come with multiple downstream risks. Changing your mind about an ECCN, without documenting the reasoning in detail, creates considerable enforcement risk.

Next, a person seeking to export an item subject to the EAR must take the relevant ECCN for the item and check the recipient's country/region:

- If an item is listed on the CCL, transferors must review the Commerce Country Chart and determine whether a license is required for the nationality of the recipient (and the destination country, if different).[17] Under the EAR, for individuals, nationality is determined by the individual's ***most recent*** country of citizenship or permanent residence, except that a person holding U.S. citizenship is always a U.S. person and exempt from these controls.
- If an item is classified EAR99, then Part 746 of the EAR must be checked, which covers the specific embargoes on Iran, Syria, North Korea, Crimea, Donetsk, Luhansk, Russia, and Cuba. Technology classified under 9E991 is subject to AT controls, which also require review of Part 746, and such technology generally requires a license for delivery to Iran, Syria, North Korea, Crimea, Donetsk, Luhansk, Russia, and Cuba.

Third, apart from country-level controls, transferors must also consider end use and end user controls under Section 744 of the EAR. These controls restrict transfers to specific parties, either for specific uses or because of the identity of the party, regardless of the party's nationality. As discussed in detail below, the U.S. government has greatly expanded the use of end user controls under the EAR, which require licenses for certain transfers to specific entities or categories of persons. In practice, companies should inquire as to the specific end user when transferring controlled items. If the end use cannot be known at the time of export, companies should ensure that respective export controls and compliance provisions are incorporated into the relevant contract, purchase order, or agreement.

As described above, a deemed export and deemed reexport can occur if controlled technology is shared to a foreign person within the United States or to a third-country national overseas. For example, a U.S. exporter transfers controlled proprietary technology to a firm in Country A. The firm in Country A employs an individual from Country B who is not a permanent employee of the firm in Country A. The release of the U.S.-origin controlled proprietary technology to the

[15] 15 C.F.R. § 734.16.

[16] *See* Supplement No. 1 to 15 C.F.R. Part 774.

[17] Supplement No. 1 to 15 C.F.R. Part 738.

employee would constitute a release to Country B; therefore, prior to releasing such technology, the firm in Country A would need to determine whether a license is required to send the technology to Country B. BIS has imposed penalties on deemed exports and reexports in the past.

Importantly, under the EAR, the foreign person's most recent country of citizenship or permanent residency is to be analyzed for licensing purposes. Meanwhile, under the ITAR, the foreign person's past and current citizenship or permanent residency are considered.

If a license is required for a specific export (for example, to a national of a certain country or an end user), then there may be an applicable "license exception." For example, License Exception RPL permits the transfer of most items subject to the EAR to most destinations for the provision of certain maintenance and repair services, if a set of procedures are followed.[18] If a license exception applies, there is no need to submit an application and wait for a determination by the U.S. government to complete the export — the exporting company must simply follow the relevant procedures to ensure the requirements in the regulations are met. Parties are allowed to rely on exceptions without affirmative approval from BIS, provided their own analysis confirms that the regulatory requirements in EAR Part 740 are satisfied.

II. ITAR

The ITAR is administered by the DDTC and regulates the export (including "deemed" exports), reexport, and transfer (in-country) of "defense articles" and "defense services" from the United States to any foreign destination or foreign person (whether located in the United States or abroad) and requires U.S. entities to comply with registration, licensing, recordkeeping, and reporting requirements.

A product or service and its related documents are deemed to be defense articles subject to the ITAR when they are enumerated on the United States Munitions List (USML). The USML is included in the ITAR and lists the defense articles and defense services that are subject to the ITAR.

Defense Article. "Defense Article" means any item or "Technical Data" designated on the USML. The term includes "Technical Data" recorded or stored in any physical form — including models, mockups, or other items — that directly reveal Technical Data related to items designated on the USML. It also includes forgings, castings, and equivalent additive manufacturing of other unfinished products, such as extrusions and machined bodies, that have reached a stage in manufacturing where they are clearly identifiable as defense articles by their mechanical properties, material composition, geometry, or function. It does not include basic marketing information on function, purpose, or general system descriptions.

Defense Service. "Defense Service" means:

1. The furnishing of assistance (including training) to foreign persons — whether in the United States or abroad — in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;

[18] 15 C.F.R. § 740.10. Use of License Exception RPL is subject to certain limitations and conditions. For example, the Item subject to License Exception RPL must have been originally exported or reexported under a license or authorization granted by BIS or an authorization, e.g., a license or exemption. Further, parties must ensure appropriate records related to use of License Exception RPL are maintained in accordance with EAR requirements.

2. The furnishing to foreign persons of any Technical Data, whether in the United States or abroad; or
3. Military training of foreign units and forces — regular and irregular — including formal or informal instruction of foreign persons in the United States or abroad; correspondence courses; technical, educational, or information publications and media of all kinds; training aids; orientation; training exercise; and military advice.

With limited exception, authorization from DDTC is required for the export, reexport, or in-country transfer of any defense article or defense service on the USML and related technical data, including any transfer to foreign persons (including employees) within the United States.

Under the ITAR, all exporters, brokers, and manufacturers of defense articles and defense services, as defined by the ITAR, must register with the DDTC. The registration forms, related materials, and registration instructions are available on the DDTC website. The registration fee varies depending upon the company's need for licenses. DDTC registration must be renewed annually. A reminder notice is sent to registrants at least 60 days prior to the expiration of the current registration; however, the registrant is responsible for ensuring that the registration is renewed and the fees are received before the expiration date, which is included on the registration letter issued by the DDTC.

Unless an exemption applies, a license or other approval is required to export ITAR-controlled items listed on the USML or to perform Defense Services. DDTC Registration does not constitute authorization to engage in ITAR activities. Counsel may be consulted through the Export Compliance Teams prior to determining whether a license exemption applies to a specific export and/or activity.

Most authorizations under the ITAR come under three headings:

- *License.* This is a document issued by the DDTC, which permits the export (or temporary import) of a specific defense article or defense service controlled by the USML.
- *Agreement*. This is an agreement, approved by the DDTC, for the performance of defense services (such as training), the disclosure of technical data to a foreign person, or the grant to a foreign person of the right to manufacture or distribute defense articles.
- *Exemption.* This is an authorization granted under the ITAR for the export of certain defense articles without additional approval from the DDTC (e.g., ITAR 123.16), although a report of any export transactions covered by the exemption is often still required.

Export authorizations, such as licenses and agreements, must be requested and approved *in advance* from the DDTC. The time required for some U.S. government approvals can be three or four months, or even longer in some cases.

III. Economic Sanctions

The U.S. Treasury Department's OFAC is primarily responsible for defining and administering U.S. sanctions programs.[19] The U.S. Commerce Department and the U.S. State Department

[19] The OFAC website is available at: http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx.

also play a role, particularly in the terrorism and narcotics trafficking sanctions regimes, under the Iran Sanctions Act, and in implementing controls on U.S.-origin goods, software, and technology. The U.S. State Department is primarily responsible for the administration and implementation of Helms-Burton (secondary sanctions on persons who "traffic" in property confiscated in Cuba from U.S. persons), the United States' "secondary sanctions" targeting Iran,[20] and certain sanctions targeting business with the Russian military and intelligence sectors. The State Department, the Commerce Department, and OFAC also jointly implement a wide range of sanctions and export controls involving Russia, including secondary sanctions targeting ongoing support for Russia's war in Ukraine. OFAC's regulations for each targeted country are broadly drafted; OFAC's oldest sanctions programs tend to be the broadest.

These restrictions are in addition to those imposed under the ITAR and the EAR. While both export controls and sanctions aim to restrict trade, export controls focus on regulating the movement of specific goods and technologies, whereas sanctions are broader, targeting entire economies or specific entities to advance foreign policy or national security objectives. In practice, companies' compliance programs must account for both regimes and ensure adequate screening measures are in place.

The United States implements three types of sanctions: (1) geographic (country/region-based) sanctions; (2) "List-Based" Programs; and (3) secondary sanctions applicable to non-U.S. persons.

Country/Region-Based Sanctions. The United States imposes restrictions on transfers subject to U.S. jurisdiction with specified countries and regions. As of the date of this memorandum, these include Cuba, Iran, North Korea, and three regions within Ukraine (Crimea, Donetsk, and Luhansk). The United States also imposes restrictions on transfers and certain dealings with the government of Venezuela and Venezuelan government-owned entities.

OFAC's "List-Based" Programs. Most of OFAC's sanctions programs may appear to be based on geography — such as those involving the "Balkans" — but they primarily result in list-based designations rather than broad, countrywide sanctions. From a U.S. perspective, these are "smarter," more targeted sanctions. Under this model, instead of prohibiting transactions with an entire country, OFAC instead designates the individual entities or individuals with which U.S. persons may not deal or impose restrictions. This "list-based" model has been used both for sanctions programs targeting countries and for programs targeting specific types of activities. The sanctions programs sometimes use a designation of "-Related" to signify that the sanctions do not target a geographic area (such as the Balkans), but rather individuals from those areas engaged in activities contrary to U.S. national security or the foreign policy interests of the United States and its allies. Some also focus on specific activities such as cyber intrusions, election interference, proliferation, transnational crime, etc.

We list below the countries and activities subject to this type of "list-based" program:

- Afghanistan-Related Sanctions
- Balkans-Related Sanctions
- Belarus Sanctions

[20] We use the term "secondary sanctions" to refer to U.S. sanctions that target one country, but do so by threatening to impose U.S. sanctions against third-country companies that engage in conduct that U.S. law defines as "sanctionable."

- Burma-Related Sanctions
- Central African Republic Sanctions
- Chinese Military Companies Sanctions
- Countering America's Adversaries Through Sanctions Act of 2017 (CAATSA)
- Counter Narcotics Trafficking Sanctions
- Counter Terrorism Sanctions
- Cuba Sanctions
- Cyber-Related Sanctions
- Democratic Republic of the Congo-Related Sanctions
- Ethiopia-Related Sanctions
- Foreign Interference in a United States Election Sanctions
- Global Magnitsky Sanctions
- Hong Kong-Related Sanctions
- Hostages and Wrongfully Detained U.S. Nationals Sanctions
- International Criminal Court-Related Sanctions
- Iran Sanctions
- Iraq-Related Sanctions
- Lebanon-Related Sanctions
- Libya Sanctions
- Magnitsky Sanctions
- Mali-Related Sanctions
- Nicaragua-Related Sanctions
- Non-Proliferation Sanctions
- North Korea Sanctions
- Rough Diamond Trade Controls
- Russian Harmful Foreign Activities Sanctions

- Somalia Sanctions
- Sudan and Darfur Sanctions
- South Sudan-Related Sanctions
- Transnational Criminal Organizations
- Ukraine-/Russia-Related Sanctions
- Venezuela-Related Sanctions
- Yemen-Related Sanctions
- Zimbabwe Sanctions

OFAC's list of sanctioned persons is quite long. It includes Specially Designated Nationals (SDNs)[21] both for OFAC "list-based" programs and for OFAC countrywide programs. It also includes persons who are not SDNs but are nevertheless subject to sanctions. In some cases, an SDN designated under one of OFAC's country-specific sanctions programs may actually be a citizen and resident of another country. The list can be found on the OFAC web site at http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx.

The consequences of being listed on the SDN List are threefold: First, all property of a listed SDN that comes within the possession or control of a U.S. person, or within the territory of the United States, is "blocked"; second, because most dollar-denominated interbank funds transfers clear through banks in the United States, SDNs are essentially denied the ability to initiate or receive dollar-denominated funds transfers; third, no U.S. person can engage in any transaction or dealing with a listed SDN.

OFAC also maintains several other lists, such as the Ukraine-/Russia-related Sectoral Sanctions Identifications (SSI) List, which involves sanctions restrictions that fall short of full blocking sanctions.[22] Individuals or entities appearing on the SSI List are subject to certain targeted restrictions that appear in "directives," predominantly involving prohibitions on transactions and dealings related to the extension of credit to SSIs. For any SSI listing, OFAC publishes the specific, applicable restriction along with the identifying information on the listing.

50 Percent Rule. OFAC applies the rule that, once a person or entity has been designated an SDN, any entity that is owned 50% or more by the SDN is deemed automatically "blocked" as a matter of law, even if its name does not appear on the SDN list. This automatic blocking thus cascades down the corporate chain to block second, third, and lower-tier subsidiaries that are ultimately owned 50% or more by the originally designated SDN. OFAC "aggregates" the ownership interests of different SDNs in determining whether an entity is blocked. Thus, if one SDN owns 25% of Company A, and another SDN owns 35% of Company A, Company A is automatically considered an SDN.

---

[21] The abbreviation "SDN" stands for "specially designated national." These are persons, either individual or corporate, that are subject to OFAC sanctions. SDNs are more fully discussed below under the heading "OFAC's 'List-Based' Sanctions."

[22] Additional partial restrictions include certain investment-related restrictions for companies identified on the Non-SDN Chinese Military-Industrial Complex Companies List (the "NS-CMIC List").

The baseline rule is that, once an entity has been determined to be an SDN, it is treated as if it was 100% owned by an SDN. Thus, if that entity owns 50% of a subsidiary, that subsidiary is likewise considered an SDN (even if the entity itself is only owned 50% by one or more SDNs). By the same token, however, if an entity is owned less than 50% by one or more SDNs, that entity is not considered an SDN and its ownership of any subsidiary, regardless of percentage, is ignored in conducting the analysis under OFAC's 50 percent rule.[23] This rule applies equally to SDNs as well as to Russia/Ukraine SSI List entities, which are not subject to U.S. prohibitions on all trade, but may be subject to restrictions on financing and transfers of certain types of technology.

Taken together, companies must invest in adequate screening measures and conduct appropriate due diligence on their investors, vendors, suppliers, and customers. There are several proprietary tools in the market that are used within the industry to automate and conduct this screening.

IV. CFIUS

CFIUS is an interagency committee[24] authorized to review certain transactions involving foreign investment in the United States in order to determine the effect of such transactions on the national security of the United States. CFIUS operates pursuant to Section 721 of the Defense Production Act of 1950, as amended ("Section 721"), and the Treasury Department's implementing regulations at 31 C.F.R. part 800. As the President's designee under Section 721, CFIUS has the authority to recommend that the President block or unwind investments subject to statute based on concerns for U.S. national security.

Traditionally, CFIUS' authority to review private transactions was limited to certain "covered [control] transaction[s]," defined as "any merger, acquisition, or takeover . . . by or with any foreign person which could result in foreign control of any person engaged in interstate commerce in the United States."[25] CFIUS' jurisdiction was thus limited to reviewing transactions involving "U.S. businesses,"[26] even if the target's U.S. operations were only a part of a larger international business. Notably, prior to the enactment of the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), CFIUS had jurisdiction to review only transactions that could result in "control" of the U.S. business by a foreign person. Control in this context, however, did not necessarily require that the foreign person acquire a majority interest in the U.S. business; CFIUS' regulations clarified that minority interests that conferred a significant ability to influence "important matters" related to the U.S. business could also confer control.[27]

---

[23] For more information on how OFAC applies the aggregate 50 percent rule, please see OFAC Frequently Asked Question #401, https://ofac.treasury.gov/faqs/401.

[24] CFIUS member agencies include: the Departments of Treasury (chair), State, Defense, Justice, Commerce, Energy, and Homeland Security; the Office of the United States Trade Representative; and the Office of Science and Technology Policy within the Executive Office of the President. The Office of the Director of National Intelligence and the Department of Labor are *ex officio* members, and five White House offices are observers.

[25] See Defense Production Act of 1950, Section 721.

[26] CFIUS had interpreted the definition of "U.S. businesses" to cover only businesses that have some form of fixed place of business in the United States, which may be an office or collection of assets. But the 2018 amendment to the CFIUS statute broadened CFIUS' statutory jurisdiction by changing the definition from an entity "engaged in interstate commerce in the United States, but only to the extent of its activities in interstate commerce" to simply "a person engaged in interstate commerce in the United States." 31 C.F.R. § 800.252. This definition is discussed in greater detail below.

[27] These "important matters" include, but are not necessarily limited to: the sale, transfer, or encumbrance of principal assets; merger and dissolution; the closing of facilities; major expenditures; the selection of business lines; the entry

FIRRMA broadened the authorities of the President and CFIUS under Section 721 in several ways, including by expanding the scope of foreign investments subject to review to include certain investments *even if they do not result in foreign control of a U.S. business.* Specifically, FIRRMA added to Section 721's "covered transactions" any "covered investment" (i.e., a non-controlling investment) by a foreign person — unless that foreign investor is "excepted," as explained below — in a U.S. business involving "critical technology," "critical infrastructure," or "sensitive personal data" (otherwise known as a "Technology, Infrastructure, or Data" business, or "TID US business"). In addition, CFIUS also now has jurisdiction over covered real estate transactions,[28] transactions structured to evade or circumvent CFIUS review,[29] and changes in the rights that a foreign person has with respect to a U.S. business if they result in control of a non-passive investment.

FIRRMA also sets forth a number of procedural reforms to the CFIUS review process, including, as discussed above, mandatory declarations in certain instances. Prior to the enactment of FIRRMA, parties typically *voluntarily* submitted notices of transactions to CFIUS – though CFIUS had, and continues to have, the authority to review pending or completed transactions even absent a voluntary notice if a member has reason to believe the transaction is subject to CFIUS jurisdiction and may raise national security concerns. Regardless, FIRRMA essentially implemented three types of CFIUS review: (1) voluntary notices (the primary form of CFIUS filing prior to the enactment of FIRRMA); (2) voluntary declarations; and (3) mandatory declarations.

While there is no list of "triggers" that CFIUS considers before reviewing a proposed transaction, some situations make a review more likely: (1) acquisitions that would result in foreign control over U.S. TID businesses; (2) lending arrangements that give the foreign party an interest in the profits of a U.S. business; (3) the foreign acquisition of a U.S. business that is involved in defense contracts with the U.S. government; and (4) real estate transactions near sensitive military installations and ports. Practically speaking, companies engaging in transactions that involve some global nexus should contact an attorney to evaluate the transaction for potential CFIUS implications. Furthermore, while a filing to CFIUS may not be mandatory, it may be a matter of best practice to submit a filing in order to avoid more onerous inquiries or requirements after the transaction has been completed.

---

into or nonfulfillment of contracts; proprietary information policy; the appointment of senior managers or employees with access to sensitive information; and the amendment of the business's governing document. 31 C.F.R. § 800.208.

[28] Under FIRRMA, CFIUS has jurisdiction over certain types of real estate transactions that do not also involve the acquisition of an interest in a U.S. business. A "covered real estate transaction" is any purchase or lease by, or concession to, a foreign person of covered real estate that affords that person at least three of the property rights identified in the regulations (such as ability to physically access the real estate). In turn, "covered real estate" includes that which is located in the United States and (i) is located within or will function as part of an air or maritime port or (ii) is in close proximity to, among other locations, a U.S. military installation. 31 C.F.R. §§ 802.211, 802.212.

[29] This latter point will not be discussed in any additional detail, but includes, for example, a situation which a foreign-owned company transfers money to a U.S. citizen who agrees, pursuant to an informal arrangement, to engage in transactional activity on behalf of that company with a view towards circumvention.

Impact on Startups

Restrictions and requirements under U.S. export controls and sanctions often appear to be antithetical to the foundational tenets of traditional startup culture. Startups typically seek to foster a fast-paced culture of collaborative development focused on cutting-edge technology and real-time solutions. In contrast, U.S. export controls and sanctions place limits and restrictions on what commodities, software, and technology may be sent to certain locations and/or provided to certain persons, often subject to months-long review and consideration by U.S. government officials. This inherent tension has historically caused startups to discover violations of U.S. law after the fact, leading to unnecessary liability risks and legal costs. Thus, U.S. and non-U.S. startups must take steps to determine if they are subject to U.S. laws and, if so, ensure they remain ensure ongoing compliance.

I. Jurisdictional Determination

Determining if an organization is subject to U.S. export controls and sanctions is a somewhat complex analysis because different legal regimes apply both within and outside of the United States. As an easy rule, these legal regimes apply to "U.S. persons," which for natural persons (i.e., individuals) generally means U.S. nationals, permanent residents, and certain protected persons. With respect to companies and other legal entities, an entity qualifies as a "U.S. person" when it is organized or exists (e.g., is incorporated) under the laws of the United States. It also includes any governmental (federal, state, or local) entity.

The business or other activities of a non-U.S. company may also qualify as the activity of a U.S. person, depending on who is directing or performing the activity. Both the ITAR and the EAR place restrictions on activities performed by U.S. persons, even if such activities are conducted abroad and without any other U.S. nexus. Furthermore, if a U.S. employee acts on behalf of a non-U.S. company in violation of applicable U.S. export controls and sanctions, a non-U.S. business may be liable for "causing" that employee to violate U.S. law. Similarly, if a non-U.S. employee is temporarily located in the United States for work or vacation travel, then the actions of the employee will be considered the acts of a U.S. person, and any violations of U.S. export controls and sanctions could be attributed to the non-U.S. company.

U.S. export controls and sanctions restrictions have wide ranging extraterritorial reach as both the ITAR and the EAR regulate "reexports" – the actual shipment or transmission of items subject to the EAR from one non-U.S. country to another non-U.S. country. Therefore, any company that engages with items subject to U.S. export controls must be aware that just because the item is outside of the U.S. does not mean the laws no longer apply. In other words, the laws follow the goods.

II. Basic Requirements for Compliance

To ensure compliance, the U.S. government generally expects companies to develop and implement an effective Export Compliance Program (ECP), which consists of a series of

procedures to help organizations operate export activities in accordance with U.S. law. The following elements should build the foundation of an ECP but are by no means exhaustive: (1) assessing risk; (2) managing export authorizations; (3) recordkeeping; (4) training; and (5) conducting audits and compliance reviews. These elements should be tailored to the size of the organization; the strategic nature of the items designed, developed, and exported; the geographic location of the organization, customers, and business partners; and the volume of exports.

As a starting point, management commitment is crucial, as compliance is more likely to be fully embraced within an organization when requirements are clearly communicated and have effectively flowed down. Furthermore, management dictates the priorities of a company, including staffing, training, and resources. Starting early and investing in a compliance program that assesses an organization's risks will mitigate any vulnerabilities. If ignored, export compliance risks can negatively affect an organization's reputation and business; therefore, companies should identify potential areas of concern and develop appropriate safeguards in advance. Some of the most common risks include exporting items without proper authorization and releasing sensitive or controlled technology without the required approval. Therefore, it is imperative that companies assess all products, software, or technology that they develop, procure, or otherwise receive in order to ensure such items are properly controlled.

Jurisdiction and Classification. When classifying an internally developed item or technology, the characteristics, technical specifications, or capabilities of the item or technology should be reviewed against the parameters identified as controlled within appropriate USML and CCL categories. When reviewing a USML or CCL entry, the Category or ECCN heading, the list of items controlled, and all technical notes should be examined. U.S. export controlled-products, software, technology, or materials that do not conform to any of the listed requirements detailed under the various categories of the CCL are designated as EAR99. Although still subject to the EAR, EAR99 items generally carry fewer restrictions than items assigned a specific ECCN.

Technology, software, components, and materials that are sourced or procured, used, stored on systems, or distributed by companies must also be classified for U.S. export controls compliance purposes. This information should be requested from the supplier. Vendors may already make this information freely available online or provide general points of contact for obtaining such jurisdiction and classification information. If a vendor classification is obviously incorrect, it must not be relied upon blindly. The Export Classification Form (Annex 3) can be used when new products or technology are being supplied.

Authorizations. Once a company knows the classification of its items, it can evaluate the necessary authorizations it may need. Although not all transfers involving foreign persons or foreign locations require advanced approval from the U.S. government, each prospective transfer should be reviewed to ensure that all legal requirements are met prior to export. This includes reviewing the particular counterparties, activities, and countries/territories associated with such transactions and comparing this information to the applicable list, activity, or country/territory-based controls — including a search against the various DDTC, BIS, and OFAC lists. To the extent authorization is required, companies should follow the proper procedures outlined in the regulations to obtain it — while also considering that a license exception or exemption may be available.

Recordkeeping. Once an item is exported, it is essential to maintain appropriate records in order to comply with applicable recordkeeping requirements. The Departments of Commerce and State and the Treasury each have different recordkeeping requirements. Startups may be asked by agencies to produce their records, so it is imperative to closely adhere to the requirements.

Under the ITAR and the EAR, records are required to be maintained for most transactions (including exports, reexports, transfers (in-country), transshipment, and diversion of items) for at least five years. Examples of records that must be retained include: license applications, licenses, license exceptions/exemptions, ITAR registrations, electronic export information on the Automated Export System, bills of lading, notes, contracts, correspondence, invitations to bid, and financial records; businesses should consult the respective regulations for the full list of required documents. Although copies of records are permitted in some cases, original records should be retained wherever possible. For OFAC sanctions requirements, records must be maintained for 10 years.

Training. Training employees is essential to ensure an effective compliance program. Such training should be tailored based on the respective employee's scope of activities. It should also communicate what exactly is expected of the relevant employees. Training should be conducted for each new hire and should also be given periodically to all employees to keep everyone aware of their obligations and inform them of any updates or changes to the respective procedures. Without a robust training program, employees may make decisions without respect to their impact on the organization's compliance with applicable trade restrictions.

Audits and Compliance Reviews. To keep an effective export control compliance program, companies must assess the success of such programs. Conducting periodic audits of day-to-day operations can help judge the effectiveness of current procedures and identify inconsistencies. Audits can be tailored to certain conduct or scopes of activity — for example, at the functional level, by reviewing particular aspects of the export process such as recordkeeping, or at the program level, by comprehensively assessing an entire business unit. It is crucial that results of such audits be carefully reviewed and reported to management and other relevant stakeholders. Corrective actions should be devised to resolve any vulnerabilities. Most importantly, any violations of U.S. export control laws should be identified, investigated, and reported to the U.S. government.

Reporting Violations. As noted above, violations of export controls and economic sanctions can result in severe penalties. Therefore, it is highly recommended that companies develop internal procedures to encourage employees to raise any potential concerns. Clear instructions should be articulated on how to report suspected incidents internally and externally. Self-reporting any violations to the U.S. government affords companies substantial mitigating credit in any enforcement administrative action, reducing potential fines by 50%. Each applicable export controls and economic sanctions program specifies the exact process to report any suspected violations, but it is recommended that companies engage outside counsel in order to prepare and disclose such violations, as well as handle any additional engagement from the U.S. government.

III. Employee Travel and Hiring Considerations

Travel. When travelling abroad, even temporarily, everything you carry with you is considered an export, and as such is subject to U.S. export controls as well as any import restrictions of the countries you pass through. It is the traveler's responsibility to comply fully with export controls requirements. When taking items abroad, you need to verify whether the items are export controlled, based on both the type of items and your travel destination. Even a laptop and its underlying technology, and data or proprietary information on the device, may be controlled. In general, for most low-tech and commercially obtained items, a license will not be required unless you are traveling to a comprehensively sanctioned country. That being said, it is important to understand and plan for export controls compliance prior to departure, as a license may be required.

Export license requirements differ based on what you are carrying, where it is going, who it is going to, and how it is going to be used. Fortunately, many items may be exempted from licensing requirements through one or more license exceptions enumerated in the EAR. Understanding what is and is not subject to EAR exceptions is crucial for export controls compliance when traveling abroad. Below are commonly used exceptions under the EAR; however, each has certain conditions and requirements, which may preclude their use. Accordingly, it is essential to conduct an appropriate analysis before using an applicable exception. Common travel-related license exceptions under the EAR include:

License Exception Temporary imports, exports, reexports, and transfers (in-country) (TMP): authorizes various temporary exports and reexports of specified items to eligible destinations for eligible end uses, including exports, reexports, and transfers of:

1. certain tools of trade for use by the exporter or employees of the exporter;
2. certain technology by or to a U.S. person, or a foreign person employee of a U.S. person traveling or on temporary assignment abroad;
3. kits consisting of replacement parts or components;
4. commodities and software for exhibition or demonstration where the exporter maintains ownership of the commodities and software while abroad or where exporter's designated sales representatives maintains "effective control" over the commodities and software while abroad;
5. certain commodities to be inspected, tested, calibrated, or repaired; and
6. certain components, parts, tools, accessories, or test equipment by a U.S. person to a subsidiary, affiliate, or facility owned or controlled by the U.S. person.

License Exception Technology and Software — Unrestricted (TSU): authorizes the export and reexport of:

1. operation technology and software;
2. sales technology and software;
3. software updates (bug fixes);
4. "mass market" software subject to the Software Note (which does not include encryption software subject to the EAR);
5. release of technology and source code in the United States by U.S. universities to their bona fide and full-time regular employees; and
6. copies of technology previously authorized for export, reexport, or transfer to the same recipient.

License Exception Baggage (BAG): authorizes individuals leaving the United States either temporarily (i.e., traveling) or longer-term (i.e., leaving) to transport commodities, software, and technology as personal baggage (i.e., personal effects, household effects, vehicles, and tools of trade); however, the item must be:

1. owned by the individual or members of their immediate families;
2. intended for, necessary, and appropriate for the use of the individuals or members of their immediate families traveling with them; and
3. not intended for sale or other disposal.

License Exception Encryption commodities, software, and technology (ENC): authorizes the export, reexport, and transfer of certain encryption items classified under ECCN 5A002, 5A004, 5B002, 5D002, 5D002, or 5E002 as well as mass-market encryption items classified under ECCN 5A992.c or 5D992.c. ENC is not available for export, reexport, or transfer to Country Group E:1 or E:2 countries.

License Exception Consumer Communications Devices (CCD): authorizes the export, reexport, or transfer (in-country) of certain specified consumer communications commodities and software to eligible individuals and organizations in Cuba, Russia, and Belarus. Items eligible for License Exception CCD include consumer computers, tablets, mobile phones, and related software that meet the mass-market criteria (i.e., classified under ECCN 5A992.c or 5D992.c) or are designated EAR99.

License Exception Strategic Trade Authorization (STA): authorizes exports, reexports, and transfers (in-country) of eligible items to or within countries in the EAR's Country Group A (including South Korea) or to nationals of such countries.

These license exceptions are very technical and are subject to additional restrictions not expressed above. Therefore, employees engaging in foreign travel that may involve the carrying of or access to any controlled data while abroad should report such trips internally and receive approval.

In addition to restrictions on items and technologies, persons traveling must also take into account any prohibitions established under OFAC's regulations. Traveling to any comprehensively sanctioned country poses many concerns and needs to be carefully evaluated as certain activities by U.S. persons, including consulting services, may be restricted. Furthermore, OFAC prohibits most transactions involving persons or entities "ordinarily resident" of comprehensively sanctioned countries. Any involvement with persons or entities in these countries may require a license.

Hiring. A company's hiring practices must take into account employment of non-U.S. persons with respect to any applicable authorization requirements. Limitations on who can access technology under export control regulations must be harmonized with anti-discrimination considerations under federal law. Specifically, the Immigration and Nationality Act (INA) prohibits employers from discriminating in hiring or recruitment based on a person's citizenship, immigration status, or national origin. At the same time, companies must ensure they are compliant with export control restrictions without applying a presumption that a candidate is ineligible for a position requiring access to controlled technology based solely on citizenship.

As a general matter, U.S. export controls do not contain employment or hiring requirements, so companies must not limit jobs or recruitment based on national origin or citizen/immigration status. The U.S. Department of Justice published guidance on how to avoid discrimination under the INA when complying with export control laws in the hiring process. This guidance may be found here: https://www.justice.gov/crt/media/1287536.

High-Risk Industries

Companies across all industries need to assess the applicability of export controls and sanctions restrictions to their business. That being said, there are certain industries that, due to the nature of the technology at issue, are more likely to face heightened restrictions. This is because the U.S. government has a concerted interest in maintaining dominance and restricting foreign adversaries access to technology and items deemed pivotal to U.S, national security. A non-exhaustive list of high-risk industries include:

- Additive Manufacturing
- Military Items (defense articles)
- Drones
- Super- / Hypersonic
- Autonomous Vehicles
- Semiconductors and Other Microelectronics
- Artificial Intelligence
- Thermal Imaging
- Space and Satellites
- Remote sensing
- Robotics
- Position, Navigation, and Timing Technology
- Quantum Computing
- Supercomputing
- Global Positioning
- Directed Energy
- Human / Machine Interface
- Encryption
- Network Penetration
- Biotechnology and Gene Editing

Export controls play a central role in the U.S. government's management of geopolitical conflict and strategic competition, and the government is devoting increased resources and novel enforcement tools to uphold them. Section 1758 of the Export Control Reform Act of 2018 (ECRA) mandates that BIS identify and develop controls on emerging and foundational technologies that are "essential to the national security of the United States" (collectively,

"Section 1758 technologies"). Section 1758 technologies are identified based on (1) the development of these technologies in foreign countries; (2) the effect export controls may have on the development of such technologies in the United States; and (3) the effectiveness of export controls in limiting the proliferation of emerging and foundational technologies in foreign countries. This provides the authority for any future restrictions on technology the United States may later determine to be pivotal to national security.

Recommendations

What is a corporate leader to do with this seemingly endless, ever-changing morass of regulations? Unfortunately, there is no universally applicable answer.

One approach, favored by many practitioners in the field, is "training-based." In such a framework, the company will roll out comprehensive training to all employees, so that they can take appropriate actions and make decisions related to export controls. Our experience has been that overreliance on such systems is often a mistake, producing incoherence, ignorance, and panic among employees.

There is no clear unifying theory behind export controls. Other pieces of legislation are more amenable to a training-based approach: With the Foreign Corrupt Practices Act, the simple version of a policy is something like "Don't bribe people. Don't accept bribes. And don't do things that might seem like you're bribing someone through a third party. Act overseas like you would act in the United States, because U.S. law applies to you regarding corruption overseas. If you're unsure, contact the company lawyers." That's not a comprehensive policy — the law is complex — but that covers the *very broad* gist of how to comply.

There's no similar statement for export control law, which is a broad, ever-changing mass of individual regulations, interpretations, and bureaucratic rulings without any unifying theme.

We've seen multiple startups that tried to train their engineering teams to comply with export law by teaching them how it works. Such an approach is always tempting for leadership, since it pushes responsibility onto the employees. It also does not work. Generally speaking, the outcome of such training is organizational paralysis and bad decision making; engineers don't have the time or the desire to understand these rules, and they don't want to go to jail for making the wrong decisions. Most especially for non-U.S. citizen engineers, who are nervous about their visa status, the level of stress and panic incurred while trying to comply with these laws is enormous.

So, what is a corporate leader to do?

- Accept that these laws *do* apply to you and that a compliance program is necessary. Ignoring these laws is a mistake.
- Consider the fact that these regulations have been changing at an accelerating pace over the past few years. As you structure your business, you need to anticipate further changes to these regulations as geopolitical dynamics evolve. Design your business to take this into account.
- Factor in the legal and regulatory overhead associated with operating across multiple jurisdictions and with hiring non-U.S. person employees. When you plan your hiring and your locations, take into account that decisions about these topics can be consequential for your operations in the future.
- Keep in mind that these regulations may well determine where and to whom you can sell your product, where you can buy supplies and services, and where you can operate. The U.S. is not the only place imposing end user restrictions and export controls: China

is taking similar steps with the goods that they manufacture and export, to name just one example.

- Consider the possibility that export controls can be a source of differentiated advantage. If the rules change in a way that cripples a competitor, but you are not damaged — because you've anticipated the likely changes and designed your organization accordingly — you can use that as an opportunity for disruption and for taking market share.
- Cultivate an environment for your team where they can operate without thinking very hard about export controls.

This last point is critical. A compliance program can be broadly digested into three categories of actions: these actions should be kept extremely simple. These categories are a whitelist, a blacklist, and a greylist:

- **The Whitelist** is the list of all the actions that an employee can *always* take safely. For instance, in an organization where all employees are U.S. citizens, this could include putting design information onto a shared hard disk accessible to the entire company. In a more complex organization, there could be a shared file that is accessible only to the people who have been formally read into a given program: Employees would know that they can use this share, because only authorized people have access. Similarly, travel for business or leisure to a named list of countries could be designated as "safe" for bringing a company laptop, from an export control perspective.
- **The Blacklist** is the list of actions that must *never* be taken without explicit, written permission from the export control officer. If any of these actions appear to be occurring, they must be reported immediately, as they carry significant compliance risk. This might include any interaction with companies or individuals in embargoed jurisdictions.
- **The Greylist** is the list of actions that are operationally necessary and may occur regularly, but must be coordinated with the export control officer to determine the details of how they should be executed. This could include engaging in business with entities that require a license, where that license is fairly routine to obtain; or it could include the vetting of potential employees who are not U.S. citizens, to ensure that appropriate licenses are being obtained.

For startups — especially in high-tech, sensitive areas — it is very desirable to design the organization, the hiring strategy, the physical locations, the choice of customers, and the supply chains in such a way that the whitelist encompasses as much of the day-to-day operations as possible, the greylist only shows up occasionally in the lives of ordinary employees, and the blacklist almost never shows up. It is also critical that employees understand the clear, simple actions they should take when encountering something in their work that appears on the greylist or blacklist.

The training burden in this kind of scheme is greatly reduced: There is little need to truly understand export control for anyone other than the company's ECO and a few leadership team members who are formulating overall strategy. For the rest of the company, export control becomes another routine matter with some simple rules, similar to the corporate expense system.

Of course, successful use of a whitelist, blacklist, and greylist (or, really, any other) approach to export control compliance depends on keeping a close on eye on common pitfalls that are all too often missed by compliance professionals, regardless of the size of the business or the sensitivity of the technology at issue. In no particular order, here are 10 things that people often

get wrong in export control compliance, which — when not appropriately addressed — regularly result in compliance violations. Keep these in mind as you design your systems:

1. **"We Don't Export Anything."** One of the most prevalent mistakes in export controls compliance is that only businesses that sell products abroad need to care about these rules. For members of the startup community, this sentiment is often followed up with a similarly misplaced rationale, "*in fact, we do not even have a product to export yet*." However, and as discussed above, this view fails to account for releases of technology and other export-controlled information to non-U.S. persons (including employees) — a "deemed" export — within the United States. Further, companies without international business activities nonetheless may trigger export control considerations through various other common practices, such as international collaborations with academic institutions, employee travel with company equipment, and use of IT infrastructure with international storage locations. Don't fall into this trap.
2. **Classification Missteps.** Export classifications are hard. In fact, even large, sophisticated companies have paid tens of millions in penalties for the mistake of getting classifications wrong. The challenge is that classification often cannot be done well in a silo: a good classification exercise requires both technical expertise and legal expertise to work together to find the correct classification for a particular product. This is because classifications are written in the form of highly technical regulations. Unless you have a rare mind versed in both technology and the law, a team is often required. (And please do not try to use AI for classification – it does not work . . . yet.)
3. **Unmonitored Employee Travel.** Employees travel for work. Employees travel for vacation. When employees travel for work, they often work on said travel. When employees travel for vacation, they still often work. As a result, employee travel may result in exports and, in turn, export control violations. Companies need to know what each employee is working on and where they are doing the work.
4. **"Our Technology Is Not Sensitive."** Second (perhaps) to the sentiment that a company should not care about export controls compliance because their sales have not (yet) reached outside of U.S. borders, another prevalent view is that the technology is simply not susceptible to military use, and therefore should not be controlled. Not so. Restrictive export controls may target seemingly innocuous technology. For example, most personal electronics, including nearly every cellphone, tablet, and laptop, are considered highly controlled encryption items, which are restricted (yes, seriously) for export to nearly any destination outside of Australia, Canada, and the United Kingdom unless or until the manufacturer of the item undergoes certain export compliance processes and procedures to downgrade the classification restrictions associated with these items. More sophisticated companies regularly undergo the required processes and procedures to release products from these restrictive rules, whereas startups that use encryption technology often run the risk of inadvertently violating these requirements.
5. **Weak or Non-Existent Third-Party Screenings.** Another misstep is a common failure to conduct appropriate export controls and sanctions screening on all third parties with which a company directly or indirectly has dealings. Unsurprisingly, the U.S. government does not view this failure kindly. Appropriate steps should be taken to confirm that U.S. businesses are not restricted from doing business with their non-U.S. customers, partners, and financial institutions.
6. **Non-Compliant IT Infrastructures.** A corollary to the deemed export concern above, U.S. companies often overlook that where their technology is stored, and which

individuals and companies have access to such data, matters. Here is a common scenario: a company manufactures items subject to U.S. export controls and the technical data / technology in the company's possession is controlled. The company undertakes appropriate steps to confirm that all of its non-U.S. employees are appropriately licensed or walled off from such information. However, the company fails to realize that its IT administrators (or third-party IT service providers) also have access to such information, resulting in a risk of export control violations.

7. **Impractical Policies and Procedures.** This is a confession of outside counsel — we have often written export controls compliance policies and procedures that (much like this article) set out high-minded expectations and ambiguous directives in draft policies and procedures for company personnel to follow without a smidgen of practical instruction on how to comply with such requirements. Policies and procedures should explain what the rules are ***and*** *how to follow them*.
8. **Poor (or No) Recordkeeping.** Recordkeeping is a requirement that applies to all exporters. While broad, this requirement should be systematized to capture applicable records and permit the ready availability of such records upon request from a relevant regulator. You do not want to have to explain to enforcement officers why you cannot seem to find records relevant to export controlled activities.
9. **Inadequate Employee Training.** Employees form the backbone of a successful compliance program. They are often the first line of defense to prevent inadvertent export control violations, and are in the best position to spot potential gaps in a company's compliance practices. Accordingly, these key resources should be empowered with engaging and results-oriented compliance trainings. No box checking.
10. **(Over)Reliance on Artificial Intelligence.** This final word of caution is temporary, but necessary. The potential value of AI to export control compliance cannot be overstated; its uses could significantly reduce compliance burdens for large and small companies alike. But we are not there yet. AI does not understand (and often makes up) the rules, is quite horrible at export control classifications, and should not be trusted to conduct a third-party screening on a close relative. Avoid for now.

While assessing the need to take steps to address above issues is an important exercise, an effective compliance program should involve a wholistic evaluation of a company's business activities that trigger export control requirements. When things do go wrong, there needs to be a clear policy outlining whom to contact. In general, corporate counsel should be included in any discussions in order to take advantage of legal privilege. Discussions of possible violations should occur through a phone or verbal conversation when possible — a hotline is preferred over an email address for this reason.

Lastly, this is a topic for which it is best to engage expert counsel early. Truly expert counsel will be able to advise you not only on the law and on enforcement mechanisms, but will be able to provide realistic risk assessments and an evaluation of how much effort and operational burden should be taken on at different stages of corporate development. Counsel with a truly operational orientation, who can help you as an executive think through the consequences of different export compliance procedures, is critical in helping to design a program that will not damage the operations of the company.

Author Biographies

Trevor Schmitt

Trevor is a national security attorney in Arnold & Porter's Washington, D.C. office. His practice focuses on national security law, complex internal investigations, and government contracts with a particular focus on working with individuals and companies in government and internal investigations related export and sanctions enforcement, including with respect to the International Traffic in Arms Regulations (ITAR), the Export Administration Regulations (EAR), and Office of Foreign Assets Control (OFAC) sanctions. Trevor regularly deals with various government agencies responsible for the administration of these laws and appears before panels, courts, and other forums hearing disputes involving international trade and investment matters.

Beyond his practice, Trevor serves as vice chair of the American Bar Association's (ABA) Export Controls and Economic Sanctions Committee and co-chair of the District of Columbia Bar's International Trade Committee. He is also a recognized author, including as a contributing author to U.S. export control law articles in various leading publications such as *Bloomberg Law*, *The Computer & Internet Lawyer, The Global Trade Law Journal, The Intellectual Property & Technology Law Journal,* and *The Privacy & Cybersecurity Law Report*. Trevor has served as co-editor for the export control developments section for the ABA's annual Year in Review publication from 2024-2026.

Trevor graduated, magna cum laude, from the Georgetown University Law Center, where he was elected to the Order of the Coif. While in law school, he served as an Executive Senior Editor for *the Georgetown Journal of International Law* as well as a Managing Editor for the *Georgetown Law Technology Review*. Trevor received his undergraduate degree, magna cum laude, from the University of New Mexico, and received an Undergraduate Advanced Diploma (UGAdvDip) in Data and Systems Analysis from the University of Oxford.

Bell Johnson

Bell is an attorney in Arnold & Porter's Washington, D.C. office, where she advises clients on a wide range of national security and international trade matters, with a particular focus on export controls, economic sanctions, and foreign investment issues. She regularly helps clients navigate complex regulatory regimes administered by the U.S. Departments of Commerce, Treasury, and State.

Bell earned her J.D., magna cum laude, from Syracuse University College of Law, where she served as managing editor of the *Syracuse Law Review*. She also earned a Master of International Relations from Syracuse University's Maxwell School. Before joining the firm, she interned with the U.S. Attorney's Office for the Northern District of New York, and she previously worked in journalism and digital media.

She is involved in the national security and international trade bar, including participating in programs and events organized by the D.C. Bar's International Trade and National Security committees and the ABA's Export Controls & Economic Sanctions Committee.

Michael J. Hochberg

Michael's career has spanned the space between fundamental research and commercialization. During his time as an undergraduate in physics at Caltech, he and his collaborator, Tom Baehr-Jones, spun off an electromagnetic supercomputing simulation company called Simulant, which they eventually sold. He co-founded his second company, Luxtera, during his senior year. Luxtera was acquired in 2018 by Cisco Systems for $660,000,000.

Later, Hochberg co-founded the first silicon photonics design services company, which was acquired by a private equity firm. He co-founded Elenion, which built and shipped several generations of coherent telecommunications and datacenter transceivers before being acquired by Nokia, where he served as the CTO of Optical Subsystems. His work has been pivotal in the creation of several other companies, in areas including photonic biosensing, chip design services, optical computing, foundry-based fabrication of semiconductor devices, and electronic design automation. He served as president of an AI supercomputing hardware startup for approximately two years.

He has published numerous papers and patents, and his work has been cited over 23,000 times (Google Scholar) in the scientific literature. His articles have been published in *Science*, *Nature*, and other top scientific journals. His co-authored book, Silicon Photonics Design: From Devices to Systems, was published in 2015 by Cambridge University Press and has been widely adopted as a textbook in the field. Recently, Michael has turned his attention to policy, geopolitics, economic statecraft, and grand strategy. He has published in various outlets including *National Review Online*, *The Hill*, *RealClearDefense, Fast Company*, *American Spectator*, and *Naval War College Review*. These publications and postings are accessible at longwalls.substack.com.

Hochberg is the President of Periplous LLC, which provides advisory services on strategy, technology, and organization design, and is a visiting scholar at the Centre for Geopolitics at Cambridge University, where he is now working on two books devoted to applied geopolitics. He currently sits on the boards of the Mackinder Forum, CIROL, and the Foreign Policy Research Institute.

Annex 1:

Published / Fundamental Research Checklist

PUBLISHED/FUNDAMENTAL RESEARCH CHECKLIST		
Is all the information or software involved in your research published and generally accessible to the public through one or more of the following:	**Yes**	**No**
a) publication in periodicals, books, print, electronic, or any other media available for general distribution to any member of the public;		
b) subscriptions that are available without restriction to any individual who desires to obtain or purchase the published information;		
c) websites available to the public free of charge or at a cost which does not exceed the cost of reproduction and distribution;		
d) libraries open to the public, including most university libraries;		
e) patents and open (published) patent applications;		
f) instruction in general science, math, and engineering principles commonly taught at schools, colleges, and universities, and conveying information through courses listed in course catalogues and in associated teaching laboratories of academic institutions; or		
g) release at an “open” conference, meeting, seminar, trade show, or other open gathering, which is generally accessible by the public for a fee reasonably related to the cost and where attendees may take notes and leave with notes.		
Does the information and software involved in your research meet the following criteria:	**Yes**	**No**
a) results from basic and applied research in science and engineering conducted at an accredited institution of higher education located in the United States;		
b) is ordinarily published and shared broadly within the scientific community;		
c) is not restricted (either by written agreement or by informal understanding) for proprietary reasons or specific national security controls, or subject to specific U.S. government access and dissemination controls.		

Annex 2:

Vendor Trade Compliance Onboarding Form

It is [Company]'s policy to verify export classification information related to the purchase or supply of commodities, technology, or software (collectively, items). This is to ensure compliance with all applicable trade sanctions and export control laws and regulations, including, but not limited to, the U.S. Department of State, Directorate of Defense Trade Controls (DDTC), International Traffic in Arms Regulations (ITAR), the U.S. Department of Commerce, Bureau of Industry and Security (BIS), Export Administration Regulations (EAR), trade sanctions administered by the U.S. Department of Treasury, Office of Foreign Assets Control (OFAC), as well as any other laws and regulations, as applicable. In connection with this policy, please confirm the following:
Date:
Company/Organization Name:
Company/Organization Address:
Company/Organization URL:
Name of Item/Service to Be Supplied:
Country of origin of Product/Service:
Intermediate and ultimate end user of item:
Other parties that will be involved in the transaction (e.g. suppliers, intermediaries, customers, logistic providers, freight forwarders, storage facilities, testing facilities):

Part I: Compliance
1. I (We) will abide by all applicable U.S. export control laws and regulations for all products, software, or technology supplied to [Company] and will obtain any licenses or approvals required by the U.S. government and/or the selling country's government prior to the sale, export, reexport, or other transfer of products, software, or technology. In connection with this transaction, I (we) will abide by all applicable U.S. sanctions, including those issued by OFAC. I (We) will take no action that would cause [Company] to be in violation of these export control laws or sanctions.
2. I (We) certify that I (we) am (are) either unaffiliated with or legally distinct and independent from individuals or companies listed in the Department of Commerce's Table of Denial Orders, the U.S. Treasury Department list of Specially Designated Nationals and Blocked Persons (SDNs), or the U.S. Department of State's list of individuals debarred from receiving Munitions List items, and other applicable lists, i.e., Commerce's Entity List as well as the Denied Person/Company list of the selling country (Prohibited Lists), or are located, organized, or resident in a country or territory that is the subject or target of sanctions (currently, Crimea, Cuba, Donetsk, Iran, Luhansk, and North Korea). Entities on the Prohibited Lists include entities not directly named on the SDN list but owned 50% or more, in the aggregate, directly or indirectly, by one or more SDNs (the 50 Percent Rule). I (We) certify that any individual or entity designated on any Prohibited List or subject to the 50 Percent Rule will not be involved in any way (including, but not limited to, provision of services, communication, facilitation, approval, oversight, etc.) in the transaction.
3. I (We) agree to notify [Company] and submit a new form when/if the information provided in this document changes.
Part II: Certification & Signature
By signing this form, I certify that the information I have provided herein is true, complete, and accurate, and that I have the authority to make the representations and statements contained herein.

Signature:	Date:
Name:	
Title:	
Phone Number:	
Email Address:	

Annex 3:

Export Classification Form

Export Classification Form - *Please complete this form when new products or technology are being supplied to [Company].*
1. Original Manufacturer/Producer:
2. Is the item/service subject to U.S. export control law, including the ITAR/EAR, or other laws from the United States and other jurisdictions? (Circle the answer that applies.) YES / NO **If yes, please provide the export control jurisdiction and classification of the item/service under relevant export law (e.g., ECCN or USML Category):** Jurisdiction: _____ Classification: _____

Annex 4:
Foreign Transaction Reporting Form

[Company] Foreign Transaction Reporting Form - *Although not all transactions involving foreign persons or foreign locations conducted by [Company] require advanced approval from the U.S. government, each prospective export transaction needs to be reviewed to ensure that all legal requirements are met prior to export. Please complete this form for all transactions (other than vendor or supplier transactions) involving foreign persons.*
Name of the Person Responsible for Completing This Form:
Title:
Email:
Function in the Company:
Date:
Name of Customer or Third Party:
Address of Customer or Third Party:
Is This a New Customer or Third Party?: (Circle the answer that applies.) YES / NO
Item/Software/Product to be Furnished:
Export Control Information (ECCN) - If Known:
Country of Intermediate and Ultimate Destination of Item, If Applicable:
Intermediate and Ultimate End User of Item:
Intermediate and Ultimate End-use of Item:
Brief Description of the Transaction:
Other Parties that Will Be Involved in the Transactions (E.g. Suppliers, Intermediaries, Customers, Logistic Providers, Freight Forwarders, Storage Facilities, Testing Facilities):

Once completed, this template must be sent to your Compliance Officer.