Understanding the OFAC Sanctions Laws: Requirements for U.S. Companies

12.18.2020

Click here for a printer friendly version.

For ?OFAC Sanctions Requirements For Foreign Companies? See HERE.

It seems almost every day there are reports of new developments under the U.S. sanctions laws. Yet many U.S. companies do not understand the significance of these laws. While they often appear to affect distant countries such as Iran and N. Korea, they actually impact U.S. companies on a day-to-day basis. Due to the severe civil and criminal penalties involved (including recent penalties of over $1 billion), it is important for companies and their counsel to understand these laws.

The U.S. sanctions laws are a set of legal requirements designed to achieve U.S. foreign policy and national security goals. They are administered by the Office of Foreign Assets Control (?OFAC?) within the U.S. Treasury Department, in conjunction with the State Department and other U.S. agencies. Sanctions are typically initiated by the President issuing an Executive Order declaring a national emergency under the International Emergency Economic Powers Act (?IEEPA?), the National Emergencies Act or similar authority and designating the parties targeted for sanctions. While originally adopted to freeze assets of enemies in times of war, they have evolved into a powerful tool for advancing U.S. foreign policy interests around the world.[1]

Sanctions are typically imposed to force foreign adversaries to change bad behavior ? such as developing nuclear weapons or terrorist activity.[2] They frequently take the form of prohibitions on U.S. parties entering business transactions with targeted countries or individual parties, and blocking assets of targeted parties. They apply to U.S. and certain foreign companies including exporters, financial institutions, companies in effectively all industries and even non-profit organizations. As a result, they

have a direct impact on activities of many U.S. and foreign businesses.

One of the most controversial parts of the sanctions laws is that the U.S. can designate a foreign party (an individual or entity) for sanctions. Targeted parties are placed on the OFAC List of Specially Designated Nationals and Blocked Persons (the ?SDN List?) or other OFAC restricted party lists. If a party is listed on the SDN List, parties subject to U.S. jurisdiction are prohibited from entering most types of business transactions with the targeted party anywhere in the world, and the targeted party is cut off from the dollar-denominated U.S. financial system. In addition, U.S. persons are required to block the assets of the targeted party that come within the U.S. person?s possession and not deal in them. OFAC typically adds up to a thousand or more parties to the sanctions lists each year and more are being added every day - these requirements create huge compliance challenges for U.S. companies conducting international business transactions.

Requirements Under the Sanctions Laws

The sanctions laws are a collection of 35 separate regulatory programs - a list of the current OFAC sanctions programs is set forth below. The terms of each sanctions program are different and each one must be considered separately.[3] Due to the incremental nature of the programs, they are amended frequently, sometimes weekly, and require regular compliance monitoring by U.S. companies[4] A listing of the current U.S. sanctions programs is as follows:

Country-Based Sanctions Programs

- Balkans-Related Sanctions
- Belarus Sanctions
- Burundi Sanctions
- Central African Republic Sanctions
- Chinese Military Companies Sanctions
- Cuba Sanctions
- Democratic Republic of the Congo-Related Sanctions
- Hong Kong - Related Sanctions
- Iran Sanctions
- Iraq-Related Sanctions
- Lebanon-Related Sanctions
- Libya Sanctions
- Mali-Related Sanctions
- Nicaragua-Related Sanctions
- North Korea Sanctions
- Somalia Sanctions
- Sudan and Dafur Sanctions
- South Sudan-Related Sanctions

- Syria Sanctions
- Syria-Related Sanctions
- Ukraine/ Russia-Related Sanctions (including the Crimea Region of Ukraine)
- Venezuela-Related Sanctions
- Yemen-Related Sanctions
- Zimbabwe Sanctions

Policy-Based Sanctions Programs

- Blocking Property of Certain Persons Associated with the International Criminal Court Sanctions
- Countering America?s Adversaries Through Sanctions Act of 2017 (CAATSA)
- Counter Narcotics Trafficking Sanctions
- Counter Terrorism Sanctions
- Cyber-Related Sanctions
- Foreign Interference In A United States Election Sanctions
- Global Magnitsky Sanctions
- Magnitsky Sanctions
- Non-Proliferation Sanctions
- Rough Diamond Trade Controls
- Transnational Criminal Organizations

Country-Level and Policy-Level Programs. Certain of the sanctions programs are focused on individual countries (the ?country-level programs?), while others target specific activities on a global basis such as terrorist and non-proliferation sanctions (the ?policy-level programs?). Under a number of the country-level programs (such as Iran, Syria, N. Korea, Cuba and the Crimea region of Ukraine ? the ?comprehensive sanctions programs?) U.S. persons are prohibited from entering into effectively all business transactions with the targeted country, its government and its nationals, including the export and import of products, technologies and services, payments and investments, subject to exceptions described below.[5] For other country-level programs, such as Russia, Ukraine and Venezuela, certain business activities within the country are prohibited but others are permitted (the ?partial sanctions programs?). For example under the Venezuela sanctions program entering transactions with the Government of Venezuela and certain Venezuelan government-owned entities (including Petroleos de Venezuela, SA) are prohibited (along with other restricted activities), but certain other business activities in Venezuela are allowed. In certain cases the program may impose restrictions on sectors of a country?s economy, such as restrictions in the energy, financial services and defense sectors in Russia.

The current program for Russia/Ukraine is an excellent example of a partial sanctions program. In response to Russia?s invasion of Ukraine, President Obama initially imposed sanctions on a small number of Russian political leaders. When Russia continued military actions in Ukraine, the sanctions

were expanded to a wider group of political and business leaders and Russian companies (including a number of well known Russian ?oligarchs?), and a total embargo on business involving the Crimea region of Ukraine. Eventually the U.S. placed restrictions on entering certain transactions with targeted Russian companies in the energy, financial and defense sectors, although many other types of business activities in Russia are still permitted. During this period, the Bureau of Industry and Security (?BIS?) also imposed sanctions on Russia under the Export Administration Regulations (?EAR?) prohibiting certain activities involving Russian deepwater, Arctic and shale energy production.[6] More recently President Trump imposed additional sanctions on Russian parties for cybersecurity violations, meddling in U.S. elections, corruption and human rights abuses.[7]

There have also been significant, and growing, sanctions activities involving China even though there is not a formal country-level sanctions program for China. These include: (i) the designation of multiple Chinese companies and banks on the SDN List for facilitating sales to N. Korea, Iran and Venezuela; (ii) the U.S. ban on investing in securities of certain public Chinese companies with ties to the Chinese military;[8] (iii) the recent Executive Order on Securing the Information and Communications Technology and Services Supply Chain (which imposed restrictions on the purchase of assets of the Chinese social media companies TikTok and WeChat);[9] (iv) the issuance of the Xinjiang Supply Chain Business Advisory advising U.S. companies of the risks of entering transactions with Chinese companies engaged in human rights abuses targeting the Uyghurs Muslim minority group in the Uyghur Autonomous Region;[10] and (v) the adoption of sanctions involving Hong Kong under the Hong Kong Autonomy Act and Hong Kong Human Rights and Democracy Act. Thus sanctions requirements can find their way into many different types of business transactions around the globe.

Under the policy-level sanctions programs, the U.S. targets individuals and entities located in any country who have engaged in activities contrary to U.S. policy goals such as corruption, human rights abuses, nuclear proliferation and terrorist attacks. The targeted parties are placed on restricted party lists and subject to transaction blocking and asset freezes for assets subject to U.S. jurisdiction.

Targeting of Individual Persons and Entities. As referenced above, a major component of the U.S. sanctions program is that OFAC often targets individual persons and entities for the imposition of individual sanctions. Targeted parties are placed on the OFAC SDN List and all property and property interests of the targeted parties are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in.[11] As a result, U.S. persons and foreign parties subject to U.S. jurisdiction are prohibited from entering effectively all types of business transactions with the targeted party anywhere in the world. In addition, such persons are required to block the assets of the targeted party that come within such person?s possession, not deal in such assets and file initial and annual blocking reports with OFAC. In addition to the SDN List, OFAC maintains seven other restricted party lists which place different, sometimes less restrictive, requirements related to listed parties.[12]

The OFAC restricted party lists are not limited to parties from the 24 countries subject to country-level sanctions programs such as Iran and North Korea - OFAC frequently targets parties in other countries as well. Thus sanctions requirements related to SDN?s and other listed parties may arise in effectively any country in the world.

Sanctions On Entities Owned By SDNs. To further complicate matters, under OFAC policy if an entity

such as a company or partnership is owned 50% or more by one or more SDN?s, that entity is also treated as if it is on the SDN List and subject to blocking and asset freezes, even if it is not itself named on the SDN list. As such, U.S. firms are prohibited from entering business transactions with such entities. OFAC attempts to block all property and property interests of SDN parties and considers stock in an entity that is owned by the SDN (and the entity itself and its assets) as subject to the blocking and asset freeze requirements.

If a party is placed on the SDN List, the party is effectively cut off from almost all international business and financial transactions, access to bank accounts and restrictions on international travel. As a result, the restricted party lists have become a powerful tool for the United States to isolate rogue regimes, despots, terrorists and other unsavory actors, and to apply pressures to advance its interests around the world short of taking military action.

However, these requirements also create serious compliance headaches for U.S. companies to avoid entering transactions with parties subject to sanctions and companies that they own anywhere in the world in routine day-to-day business transactions. For example, when OFAC imposed sanctions on the Russian ?oligarchs? with close ties to Vladimir Putin in 2018,[13] U.S. companies had to immediately scramble to avoid sanctions violations in their dealings in Russia. These sanctions designations included many of the most prominent and politically-connected businessmen in Russia. In addition, since the sanctions also apply to companies that are 50% or more owned by these parties, the sanctions flowed down to many of the largest companies across the Russian economy that were owned by these parties including publicly traded United Company Rusal PLC, EN+, GAZ Group and Rosoboronoeksport.[14] As a result, U.S. companies that conducted business with these companies were required to quickly wind down their business dealings with these parties or risk facing penalties for sanctions violations. Now when U.S. firms are entering business transactions in Russia and Ukraine they frequently conduct detailed due diligence reviews to confirm that the Russian companies with which they are dealing are not owned or controlled, directly or indirectly, by sanctioned parties. Since many Russian companies are owned through intermediary companies, nominee shareholders, trusts or other complex structures, this creates compliance headaches for U.S. companies. These sanctions law requirements apply not just to U.S. exporters and service providers but also to private equity funds and investment partnerships, joint ventures, real estate projects, technology licensing and other business activities.

Application To U.S. and Foreign Persons. The OFAC sanctions laws generally apply to ?U.S. persons,? and in certain instances to foreign persons. The term ?U.S. person? includes: (i) U.S. citizens and permanent resident aliens wherever located; (ii) entities organized under the laws of the U.S. or a jurisdiction within the U.S. (including foreign branches of such entities); and (iii) any individual or entity physically located within the U.S. In addition, foreign subsidiaries of U.S. entities are subject to OFAC requirements under certain of the sanctions programs (for example, under the Iran and Cuba sanctions programs). Also property of foreign parties that is located in the U.S. or comes within the possession or control of any U.S. person anywhere in the world is subject to OFAC jurisdiction.

In addition, foreign persons and companies operating outside the U.S. are subject to OFAC sanctions requirements in many instances as well.[15] These include: (i) where the foreign party has a requisite

level of contacts with the U.S., such as engaging in transactions involving U.S. dollars, or dealing in U.S. products, software or technology; (ii) under ?secondary? sanctions (ie., sanctions that specifically apply to non-U.S. parties) even if the foreign party has no contacts with the U.S.; (iii) where the foreign party is designated itself for sanctions itself and listed on the SDN List or other OFAC restricted party lists; and (iv) for foreign persons providing material support or assistance to or facilitating[16] a significant transaction with certain parties that are subject to sanctions. If a foreign company or individual violates a provision of the U.S. sanctions laws, they can be exposed to significant consequences for such actions, including criminal prosecution in the U.S. and/or being designated on the SDN List themselves.[17] (For a more detailed discussion of the application of U.S. sanctions laws to foreign companies see: U.S. Sanctions Laws: Dangers Ahead For Foreign Companies.)

Evasion, Avoidance, Facilitation; Providing Material Support. Sanctions prohibitions include not just engaging in activities that directly violate the sanctions requirements, but also engaging in acts that ?evade? or ?avoid? these restrictions, and aiding, abetting and conspiracy with others to do so. Of particular note, assisting or providing material support to foreign parties in engaging in sanctions violations or evading sanctions (?facilitation?) can be a violation ? facilitation in this context is defined as assisting a foreign person in engaging in activities that would violate the sanctions laws if performed by a U.S. person.[18] Thus, even banks, accounting firms, law firms and other service providers that assist or provide resources, services or financial support to foreign parties that violate sanctions requirements or are designated as SDNs can be liable themselves for sanctions violations.

General and Specific Licenses. OFAC issues ?general? license that provide certain exceptions to the sanctions requirements such as involving information materials and the sale of agricultural products, medicines and medical devices.[19] In addition, OFAC can grant ?specific? licenses in which it provides authority for a party to engage in a particular activity that is otherwise prohibited in response to a specific request.

National Emergency Authority. Most sanctions programs are authorized under ?national emergency? authority under IEEPA, the National Emergencies Act or similar statutory authority.[20] As such, there are fewer constitutional safeguards afforded to foreign parties who are designated for sanctions[21]

Penalties and Enforcement. Penalties for violations of the U.S. sanctions laws include civil and criminal penalties of up to twenty years imprisonment and $1,000,000 in fines per violation.[22] Such penalties can be imposed on both U.S. and foreign persons. Judicial review of OFAC determinations is authorized under most of the sanctions programs, but cases are limited. The U.S. government considers sanctions violations as undermining our most important foreign policy/national security goals and consequently is very aggressive in enforcing these laws. (For additional information on penalties and steps for addressing sanctions violations see: Dealing With Violations In Export and Import Transactions).

OFAC has adopted a number of novel steps in enforcing the sanctions laws. For example, in September 2020 the Treasury Department entered into a Memorandum of Understanding with the State of Delaware to initiate joint efforts to ?shut down or otherwise disrupt the illicit activities of entities that should not be operating in the United States,? including parties on the SDN List. Similarly, in December 2020 the Trump Administration announced that it would offer a $5,000,000 reward for information

related to activities that support sanctions evasions that benefit N. Korea.

Overlap With Regulations By Other Federal Agencies. Other federal agencies have adopted requirements that overlap with the sanctions programs, including under the Export Administration Regulations (?EAR?) and the International Traffic In Arms Regulations (?ITAR?).[23] Consequently, parties should use care to review these other areas in addition to OFAC regulations when reviewing sanctions issues to obtain a complete picture of the regulatory requirements that will apply to a particular transaction.

There are also other requirements under the sanctions programs including recordkeeping requirements [24] and initial and annual reporting requirements for blocked property[25] set forth in the OFAC regulations.

Examples of recent sanctions law requirements for U.S. companies include:

- Transactions With Countries Subject to Country-Based Sanctions Programs? Restrictions *will* apply to transactions with countries subject to comprehensive country-based sanctions programs, and *may* apply to transactions with countries subject to partial country-based programs;
- Transactions With Parties On Restricted Parties Lists and Entities Owned By Such Parties? Restrictions on entering business transactions with parties listed on the SDN List and other OFAC restricted parties lists, and with entities that are owned 50% or more by one or more parties listed on the SDN List; requirements include blocking the assets of such parties and filing blocking reports with OFAC;
- Chinese Banks, Trading, Shipping and Technology Companies? Restrictions on U.S. and foreign parties in dealing with designated Chinese and other non-U.S. banks, industrial companies, trading companies, shipping companies and other business enterprises that do business with or provide financial or other support to N. Korea, Venezuela, Iran and other parties subject to U.S. sanctions;
- Cryptocurrencies ? Prohibition on entering transactions involving cryptocurrencies issued by the Government of Venezuela (including the Venezuelan cryptocurrency the ?Petro?) and other parties designated for sanctions;
- Ransomware Payments ? Restrictions on the payment of ransomware payments to cyber-criminals who have been listed on the SDN List. In addition, restrictions on companies providing support to companies making such payments including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response.[26]
- Cybersecurity ? Restrictions on entering transactions with parties that have been sanctioned for involvement in cyber-security attacks against the U.S. including N. Korean parties in the Sony Pictures cyber-attack and Russian parties in connection with the 2016 U.S. Presidential elections;
- Anticorruption ? Prohibition on entering transactions with parties designated by the U.S. for corruption violations under the Global Magnitsky Sanctions;
- Hong Kong Sanctions ? Restrictions on entering transactions with Chinese parties designated for undermining Hong Kong?s autonomy and restricting the freedom of expression or assembly of the citizens of Hong Kong pursuant to Executive Order 13936;

- Vessels - Restrictions on chartering vessels that have been designated by OFAC for participation in sanctions evasion under various sanctions programs;
- Human Rights Violations ? Restrictions on engaging in transactions with Chinese companies implicated in human rights abuses against Uyghur and other Muslim minority groups in the Xinjiang Uyghur Autonomous Region and other parties involved in human rights violations;
- International Criminal Court ? Restrictions on entering transactions with persons on the SDN List for engaging in activities involving the International Criminal Court in prosecuting or investigating U.S. persons or allies under the International Criminal Court Sanctions Program;
- High Value Artwork ? Restrictions on entering transactions involving high value artwork with parties on the SDN List, including blocking and asset freeze requirements and requirements to file blocking reports with OFAC. See OFAC Guidance document: ?Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork.?[27]
- Interference With U.S. Elections ? Restrictions on dealing with parties in Russia and other jurisdictions listed on the SDN List for engaging in activities found to interfere with U.S. elections under the OFAC Foreign Interference In A U.S. Election Sanctions Program;
- Terrorist Activities ? Restrictions on entering transactions with parties designated for sanctions for engaging in acts of terrorism, and with parties that sponsor, provide financing or material or technological support for such parties under the OFAC Global Terrorist Sanctions;
- Sanctions Evaders ? Restrictions on U.S. and foreign parties providing material support, assistance, financing and other resources for parties that are listed on the SDN List.

Sanctions Requirements In Day-To-Day Business Transactions

So how do sanctions requirements apply in your company?s international business operations? Of course, requirements may arise in one of the 24 countries subject to the OFAC country-based sanctions programs such as Iran, Syria, Russia and Venezuela, so you should be on guard when doing business in these countries. However requirements may also arise in many other countries due to restrictions on dealing with prohibited parties and entities owned by such parties on a worldwide basis (including publicly owned companies) and the risk that exports by your company to a legitimate country can be reexported by your customer to a prohibited country. Consequently it is prudent to review sanctions requirements for all countries in which you will be conducting transactions, including transactions involving exports, imports, services, licensing of software and technology, financing, investments and acquisitions, among others. The following are some examples of how sanctions requirements may arise in your company?s day-to-day business activities:

- Your company sells its product to a customer in Sevastopol, Ukraine. Since Sevastopol is located in the Crimea region of Ukraine, sales to this location are subject to a comprehensive sanctions program and prohibited unless a general or specific license applies. Similarly, restrictions *may* apply if the product is sold to a country subject to a partial sanctions program.
- Your company sells its product to a customer in the U.A.E. and the customer then resells the product to a purchaser in Iran. In this case your company could be liable for sanctions violations if

it had knowledge or ?reason to know? that the product would be resold by the customer to Iran. ?Reason to Know? is when facts were present that suggested a risk that the product would be shipped to Iran. Thus the U.S. company could have liability for a sanctions violation even if it did not have actual knowledge that the product would be resold to Iran. For further discussion of the application of the ?Reason To Know? standard see: ?Reason To Know ? A Chilling Term For Exporters.?

- Your company sells its product to a Chinese company, and the Chinese company has been sanctioned for selling products to N. Korea ? your company is prohibited from entering into any transactions with such party and must freeze any assets of that party that come into its possession.
- Your company sells industrial equipment to a customer in Europe and the customer resells the equipment to an oil and gas operator in Russia in violation of the EAR or OFAC Russian industry sector sanctions.[28] Under the terms of the EAR Russia sanctions the U.S. company is prohibited from selling the equipment if it knew that the product would be used in the Russian energy project or if it ?is unable to determine whether the item will be used in such projects.?[29] Thus your company could have liability for an EAR or sanctions violation even if it was not aware that the product would be sold to the prohibited energy project.
- Your company performs technical services for a company in the United Kingdom and this company is listed on the SDN List. You are prohibited from entering transactions with such party and are required to block its assets that come within your possession.
- Your company licenses its software to a customer that is not listed on the SDN List nor located in one of the countries subject to country-based sanctions, but its stock is owned 50% or more by a party listed on the SDN List. Since entities that are owned 50% or more by SDNs are themselves treated as sanctioned parties, your company is prohibited from entering transactions with this entity.
- You acquire a company overseas and after the closing you learn that prior to the sale the acquired company had been selling to customers in Iran, N. Korea, Syria or to parties on the SDN List, and there is a possibility that such sales are continuing. Depending on the terms of the acquisition, your company could have liability for the violations prior to the closing and almost certainly for any sanctions violations that occur after the closing.
- You sell a product to a company in Russia and you wish to obtain financing for the transaction through a Russian bank that is listed on the SDN List.[30] Since the bank is listed on the SDN List your company is prohibited from entering banking transactions with it.
- You charter a vessel that is listed on the SDN List. Since the vessel is listed on the SDN List your company is prohibited from chartering the vessel.

Sanctions requirements can arise in unexpected situations. For example, OFAC recently issued an advisory that if a company is subject to a cyber-attack by a foreign party listed on the SDN List, the U.S. company is prohibited from making ransomware payments to such party. (The advisory states that the U.S. company making the payment could be subject to liability based on strict liability, meaning that a party subject to U.S. jurisdiction may be liable even if it did not know or have reason to know it was engaging in a transaction with a sanctioned party.) The advisory further states that other U.S. parties that assist the U.S. party in making such payments, including financial institutions, cyber insurance firms, and companies involved in digital forensics and incident response, could also be liable for

facilitation.[31] In another OFAC advisory, OFAC warned U.S. companies against dealing in high-value artwork associated with persons blocked under OFAC authorization.[32]

Thus U.S. companies should use care to identify situations in which sanctions requirements may arise in the full array of their business activities.

Compliance Procedures For U.S. Sanctions Laws

What steps should your company take for compliance under the sanctions laws? OFAC recommends that companies adopt written compliance programs for sanctions law compliance. The type of compliance policies and procedures for an individual company will vary depending upon the company?s size, products/industry, countries of operation and other factors. OFAC recommends that companies conduct a risk-based analysis of their operations to identify the areas of greatest sanctions requirements and compliance risk and adopt policies and procedures focused on these risks. While every company is different and a ?one-size-fits-all? approach does not work for every company, the following are a number of compliance issues for U.S. companies to consider in dealing with OFAC sanctions requirements.

1. Transactions With Countries Subject to the Country-Based Sanctions Programs. The first issue to consider is whether you are entering a transaction with a country subject to the country-based sanctions programs. As referenced above, most transactions with countries subject to the *comprehensive* sanctions (such as Iran, Syria, Cuba, N. Korea and the Crimea region of Ukraine) are strictly prohibited unless a general or specific license applies. However countries subject to partial sanctions requirements, such as Russia, Ukraine, Venezuela, Nicaragua and Somalia (among others) may also raise significant compliance issues. In these countries, certain activities are prohibited while others permitted, requiring a careful review of the particular sanctions program in question to determine if your proposed activity is permitted. In addition, the countries subject to partial sanctions programs are likely to have a higher incidence of persons and entities that are listed on the SDN List and a greater chance that entities in these countries are owned by SDNs than in non-sanctioned countries, often warranting a higher level of due diligence review.

2. Transactions With Specially Designated Nationals And Other Restricted Parties. To protect against dealing with parties on the SDN List and other prohibited parties, companies commonly establish restricted party screening procedures. Under these procedures, the company compares parties to its transactions against the restricted party lists to confirm that the transaction parties are not named on the lists. There are many ways to conduct restricted party screening activities ? ranging from conducting manual reviews on a transaction-by-transaction basis to use of more sophisticated screening software ? the key is to adopt a screening process that is appropriate for your business.

In theory, screening for restricted parties such as SDN?s involves simply comparing the names of parties in a proposed transaction against the restricted party lists in question. However in reality restricted party screening in a modern business enterprise can be a more complex task, especially for companies selling to multiple countries, with multiple offices, products and business practices. Issues that arise include dealing with commonly used names, spelling variations, fictitious names, false positive hits and the regular addition of names to the lists. In addition to listing persons and entities on the SDN

List, OFAC also lists shipping vessels that were found to be used to evade sanctions and U.S. parties are prohibited from chartering such vessels. Similarly OFAC recently imposed penalties on a U.S. company for entering a contract with a foreign company where the executive signing the contract for the foreign company was listed on the SDN List but the foreign company was not. These and other issues complicate the screening process and make proper planning of the process important. Issues to be considered in designing a screening procedure that is appropriate for your company include:

- *Parties To Be Screened*: Companies often screen not just the parties directly purchasing their products or services but also other parties to their transactions including end users, intermediate consignees, sales representatives, agents and other intermediaries, brokers, transportation carrier(s), freight forwarder(s), banks and other parties who will perform a role in the transaction.
- *Frequency*: Companies frequently conduct screening during the activities leading up to the sale - upon receipt of the purchase order or in conducting due diligence prior to the sale. More detailed screening procedures can also used, such as batch screening of repeat customers, periodic screening following initial screening (such as on a quarterly or annual basis) and retroactive screening to cover parties that have been added to the list following the date of the initial screen.
- *Screening Procedure*: Screening can be conducted through a number of techniques including manual screening against official U.S. government restricted party lists or through use of commercially available screening software programs. For example, some companies have automated screening software build into their ERP systems to conduct screening on an automated basis, and many routinely screen all of their existing customers, vendors and other parties on a periodic basis (including retroactive screening in the event a party has been added to the list after an initial screening).
- *Search Criteria*: Companies often utilize ?fuzzy logic? or similar search techniques to screen for variations in spelling, abbreviated or fictitious names, etc.
- *Assessing Matches and False Hits*: If there is a match, the Company will need to assess if it is a true match or a false hit and communicate the results to the Company employees involved in the transaction.
- *Recordkeeping*: The company is required to maintain records of transactions subject to the OFAC sanctions requirements for a period of five years in accordance with the export recordkeeping requirements set forth in 31 CFR §501.601, and hence it would be prudent to maintain copies of the SDN screening searches.
- *Other Screening Issues*: Companies should also consider screening for shipping vessels, banks providing financial services in the transaction and individual officers of foreign companies who are signing contracts on behalf of the foreign company, among other issues.

3. Transactions With Entities Owned By SDN?s. As referenced above, under OFAC?s guidance if one or more parties listed on the SDN List own 50% or more of an entity such as a corporation or a limited liability company, the entity is also considered by OFAC to be a sanctioned party, even if the entity is not itself listed on the SDN List. Consequently U.S. persons are prohibited from entering transactions with such entity and OFAC?s blocking and freezing requirements apply[33] Accordingly, to avoid liability U.S. companies frequently conduct due diligence reviews of the stockholders of the

companies with whom they are dealing and take other compliance steps, especially if the transaction involves a country subject to heightened sanctions risk. Since it is often difficult to determine the identities of stockholders of customers and other parties to a transaction, this is one of the most challenging compliance issues in dealing with sanctions issues. Examples of compliance steps to address these issues include use of OFAC compliance questionnaires, use of export compliance clauses in transaction documents, obtaining written warranties from foreign parties regarding the identity of their stockholders, independent reviews of official records, press reports and credit reports and reviews by private investigatory firms. Each transaction is different and companies must tailor their compliance strategies to the transaction in question and the level of risk involved.

4. Unauthorized Reexports To Prohibited Countries and Parties. One of the most significant sanctions risks faced by U.S. companies is from the unauthorized reexport of its products to a prohibited country or prohibited party. Under this scenario, a U.S. company sells its product to a customer in a lawful transaction, and the foreign customer then resells the product to a party in Iran, Syria or another prohibited country or to a party on the SDN List. Such transfers could occur in a normal commercial resale by the customer or an unauthorized diversion or transshipment without the knowledge of the company. In such situation the U.S. company could have liability for sanctions violations in certain situations. For example, under §560.204 of OFAC?s Iran regulations U.S. persons are prohibited from selling products to a party in a third country with ?knowledge or reason to know? that the product will be reexported to Iran. ?Reason to know? is includes when facts are present that suggest a sufficient risk that the products will be shipped to the prohibited country.[34] Thus, even if a U.S. company does not have actual knowledge that its product will be shipped to a sanctioned country, if sufficient facts are present and the U.S. company fails to identify these in its due diligence for the transaction, the company could have a sanctions violation. (For further discussion of the application of the ?Reason To Know? standard see: ?Reason To Know ? A Chilling Term For Exporters.?) Again while a ?one-size-fits-all? approach may not work for every company, many U.S. companies conduct careful due diligence in combination with one or more of the other compliance steps described above to reduce this risk[35]

5. Other Countries Subject to Heightened Sanctions Risk. Certain countries that are not subject to specific country-based sanctions programs may nonetheless present a higher level of sanctions risk, even if they are not specifically named in a sanctions programs. This is due to being situated adjacent to countries subject to country-based sanctions programs with the increased risk of unauthorized transshipment or diversion to a prohibited country or party. Countries that are subject to such heightened sanctions risk include the United Arab Emirates, Turkey and other Middle East countries (due to proximity to Iran and Syria), China and Hong Kong (due to proximity to N. Korea), Eastern European countries (due to proximity to Russia and Ukraine) and Central American countries (due to proximity to Cuba). Also tax haven jurisdictions present heightened sanctions and money laundering risks due to their secrecy laws and lax regulatory enforcement.

6. Foreign Subsidiaries Dealing With Prohibited Countries Or Prohibited Parties. In the U.S. it is common knowledge that U.S. companies are not permitted to enter transactions with restricted countries such as Cuba and Iran. However in most foreign countries it is perfectly legal to do business with these countries. If your company has subsidiaries in foreign countries, the employees in these subsidiaries may not be familiar with U.S. sanctions laws and may engage in transactions with

sanctioned countries on a regular basis. The same principle applies in dealing with SDNs and other prohibited parties ? most foreign persons have never heard of the SDN List or OFAC screening procedures. Under certain of the OFAC sanctions programs, foreign subsidiaries of U.S. companies are permitted to engage in certain transactions with countries subject to comprehensive sanctions programs that would otherwise be prohibited for U.S. persons under certain of the sanctions programs[36] However for other country programs (such as Iran and Cuba) U.S. sanctions requirements strictly apply to the foreign subsidiaries of U.S. companies just as they apply to the U.S. parent company. To address this many U.S. companies with foreign subsidiaries provide procedures in their sanctions compliance programs for their foreign subsidiaries for complying with sanctions requirements.

7. Facilitation. As referenced above, in certain instances U.S. companies? foreign subsidiaries may be permitted to engage in transactions with countries subject to comprehensive sanctions laws[37] In such cases, however, neither the U.S. parent company nor other U.S. persons are permitted to participate in the business activities involving the sanctioned country unless authorized under OFAC licenses or other authorizations. As part of this, the U.S. parent company and U.S. person employees of the parent and the subsidiary are prohibited from providing support or resources for the foreign subsidiary involving activities in the sanctioned country such as financing, management support, U.S. products/components, U.S. technology, business leads, technical support and other resources unless such activities are permitted under the terms of general or specific licenses. Companies should be alert to these issues to attempt to avoid ?facilitation? by the U.S. parent company and other U.S. persons of such activities by their foreign subsidiaries.

In addition to activities to support foreign subsidiaries, U.S. persons should also avoid other types of activities that may constitute ?facilitation,? aiding and abetting or otherwise providing support or assistance (including financial, logistical, management and consulting support) to parties in engaging in activities that are prohibited under the sanctions laws.

8. Purchases By Foreign Customers Through Front Companies and Other Deceptive Practices If foreign business or government officials are listed on the SDN List they may consider entering transactions using fictitious names, fraudulent front companies or other deceptive practices to evade U.S. sanctions laws. They may also use complex corporate structures to hide their identities, such as holding stock through trusts, holding companies, nominee directors, use of bearer shares or similar means. This is especially prevalent in regions subject to high levels of sanctions risk such as Russia/Ukraine/Crimea, the Middle East and more recently China/N. Korea. Many companies use a heightened level of due diligence review and other compliance steps in transactions in regions subject to a high level of sanctions requirements to assure that their products/services are not unwittingly sold to prohibited end users or diverted to prohibited destinations.[38]

9. On-Line Sales. If a company engages in on-line sales or other electronic business transactions, sanctions laws frequently apply to such activities. Examples of questions to consider if your company is selling products/software or services through on-line channels include: (i) Are parties who are purchasing products/software/services from your company located in a country subject to sanctions programs such as Iran, Syria, N. Korea, Cuba and Crimea? (ii) Are parties purchasing your products listed on the SDN List or any other U.S. restricted party lists? (iii) Are entities that are purchasing your

products owned 50% or more by SDN parties? (iv) Could parties purchasing your products be reselling them to parties in sanctioned countries or to sanctioned parties? (v) Could restricted parties be using your on-line resources to evade or avoid sanctions compliance, including use of fictitious names, country locations, destinations for product deliveries, etc.? OFAC has addressed this issue of sanctions compliance for online business practices in detail in a number of enforcement cases including involving PayPal, Inc. resulting in a penalty of the $7,658,300.[39]

10. Mergers and Acquisitions. If your company is engaging in an acquisition transaction you should carefully consider OFAC sanctions issues as part of the transaction. This includes both in acquisitions of foreign companies (to review if they have engaged in transactions with sanctioned countries and parties) and U.S. companies (to review if they have lax sanctions compliance practices or past sanctions violations). If these are not handled properly your company can step into the target company?s shoes and become liable for past violations in certain cases.

If you are acquiring a foreign company questions to consider include: (i) Has the target company engaged in activities that violate sanctions laws? (ii) Does it operate in or sell products or services to countries that are subject the U.S. sanctions laws? (foreign companies often conduct business in countries such as Iran, Cuba, Syria, etc.); (iii) Does it have offices, sales agents or distributors in such countries? (iv) Has it engaged in transactions with restricted parties or entities owned by such parties? (v) Has it provided support, assistance or resources to such parties? (vi) Does your company have proper procedures to deal with sanctions issues on a post-closing basis? Such issues include requiring the foreign company to cease sales activities with sanctioned countries and parties prior to the closing of the acquisition (including activities of the foreign company and its agents/distributors in aftermarket sales support, warranty claims, collections of receivables, payments of refunds, etc.), transfers of OFAC licenses and authorizations, and remedial steps if you discover sanctions violations after the closing that occurred prior to the closing.

For acquisitions of domestic U.S. companies, the same questions should be asked as well as reviewing if the target company has proper compliance procedures in place to address sanctions issues, if has it obtained all required OFAC licenses, filed reports, complied with recordkeeping requirements and if there have been any past violations. (For additional discussion of these issues see: Acquirer Can Be Liable For Export Control Violations of Acquired Company.

The same issue often arises for U.S. companies that are looking to be *acquired in an ?exit? transaction* ? if your company has OFAC enforcement problems in its past this may scare away potential acquirers or reduce the purchase price. Thus having strong sanctions compliance procedures in place now can help to reduce the risk of such problems in the future.

11. Compliance With License Terms and Conditions, Reporting and Recordkeeping Requirements
In certain instances activities which are otherwise restricted are allowed under exceptions in the various OFAC regulations under general licenses and specific licenses. However, these licenses often have detailed terms and conditions that must be met in order to rely on the authorizations. Companies relying upon a license must conduct their activities within the terms and conditions of the authorization throughout the entire time period in which they are relying on the authorization.

12. Regulations By Multiple Federal Agencies. As referenced above, a number of other U.S. agencies administer regulatory programs that impose requirements that are similar to the OFAC sanctions laws such as the embargoes administered by the Commerce Department under EAR Part 746 and restricted party lists under Part 744, debarred party lists and trade embargoes administered by the Directorate of Defense Trade Controls (?DDTC?) within the State Department, and money laundering laws administered by the Treasury Department. Consequently U.S. companies should look beyond OFAC and monitor requirements of these other agencies as part of its sanctions compliance effort.

13. Updating Compliance Programs. OFAC recommends that companies ?routinely update? their compliance programs to keep up with changes in the law. Many companies have existing export compliance programs that were adopted years ago. However many of the sanctions requirements discussed above have been adopted within recent years, so older compliance provisions may not reflect these changes. (OFAC?s Framework for OFAC Compliance Commitments was not published until May 2, 2019.) Keeping compliance programs up to date is valuable in reducing risk for sanctions violations.

The Challenge Ahead

The U.S. sanctions laws are complex and ever-expanding. As such, they create an ongoing compliance challenge for U.S. companies. Based on current political and enforcement trends, this challenge will likely continue for the foreseeable future. U.S. companies should use care to understand these laws and adopt compliance strategies that are suitable for their business to address these issues.

Related Articles:

- EXPORT CONTROL LAWS FOR THE GENERAL COUNSEL
- DEALING WITH VIOLATIONS IN EXPORT AND IMPORT TRANSACTIONS
- ITAR FOR GOVERNMENT CONTRACTORS
- ITAR COMPLIANCE CHECKLIST

[1] OFAC, part of the Office of Terrorism and Financial Intelligence within the Treasury Department, was founded in 1950. OFAC and its predecessor agencies the Office of Foreign Funds Control and the Division of Foreign Assets Control have a history of blocking assets and restricting trade and financial transactions with U.S. enemies dating back to the War of 1812. These agencies operated under Presidential national emergency powers including under the Trading With the Enemy Act of 1917 and other statutory authority to impose asset freezes and trade embargoes involving U.S. adversaries, including administering the Proclaimed List of Certain Blocked Nationals, or the "Black List."

[2] For example, the Ukraine/Russia sanctions were imposed in response to the Russian invasion of Ukraine, and the Venezuela sanctions were imposed due to human rights abuses.

[3] There are typically separate sets of regulations, executive orders and in some cases statutory authorities for each sanctions program.

[4] In imposing sanctions under a program, the President can select from a menu of options ? ranging from a simple designation of an individual for asset blocking up to a comprehensive trade/investment ban. Sanctions are often imposed on an incremental basis for dealing with foreign affairs problems, such as the Russian encroachment on Ukraine or the Syrian use of chemical weapons. So they may initially target a small handful of parties or activities in a particular country, and if the offensive behavior continues the sanctions may be expanded to include a wider array of restrictions, sometimes culminating in a total embargo of a foreign country.

[5] In addition, the programs also block and prohibit dealing in any property interests of parties in the targeted countries who have been designated by OFAC, along with entities owned by such parties.

[6] In addition to the Ukraine/Russia sanctions administered by OFAC, the Bureau of Industry and Security within the Commerce Department maintains a number of sanctions involving Russia

including the Russian Industry Sector Sanctions set forth at 15 CFR §746.5, restrictions on dealings with certain Russian parties under 15 CFR §744.10 and restrictions on dealing with military end use and military end users in Russia under 15 CFR §744.21.

[7] In addition, as referenced above, the President may be mandated to impose additional Russian sanctions in the future under CAATSA.

[8] See Executive Order 13959: Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies, November 12, 2020.

[9] See Executive Order 13873: Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019.

[10] See OFAC Business Advisory: ?Risks and Considerations for Businesses with Supply Chain Exposure to Entities Engaged in Forced Labor and other Human Rights Abuses in Xinjiang,? July I, 2020.

[11] The U.S. may also impose other requirements under a sanctions designation such as restrictions on the issuance of visas by the U.S. to the targeted individual.

[12] In addition to the SDN List, OFAC maintains a number of other restricted party lists (plus a Consolidated List) which in some cases place different, sometimes less restrictive requirements on listed parties. These include the: Sectoral Sanctions Identifications List; Foreign Sanctions Evaders List; Non-SDN Palestinian Legislative Council List; Non-SDN Iranian Sanctions List; List of Foreign Financial Institutions Subject to Part 561 (the "Part 561 List"); the List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (?CAPTA List?); and the Non-SDN Menu-Based Sanctions List (?NS-MBS List?). OFAC also promulgates a Consolidated List which includes the identities of

parties on the SDN List and the other restricted party lists, and the US government also maintains other restricted party lists such as the BIS Entity List, Denied Persons List and the Unverified List.

[13] These included seven Russian business executives, twelve companies that they owned or controlled, seventeen Russian government officials, a state-owned weapons company and a Russian bank.

[14] On December 19, 2018 OFAC submitted its Notification to Congress of its intention to terminate sanctions imposed on United Company Rusal plc, EN+ Group plc and JSC EuroSibEnergo after thirty days as the individual party identified on the SDN List that owned 50% of such entities had restructured his ownership and reduced his holdings in such entities below 50%. On January 27, 2019 OFAC removed United Company Rusal plc, EN+ Group plc and JSC EuroSibEnergo from the SDN List.

[15] In fact, the incidence of this is increasing due to recent political events (such as in Iran and N. Korea), and legislative enactments such as the Countering America?s Adversaries Through Sanctions Act of 2017 (?CAATSA?).

[16] The concept of ?facilitation? by foreign parties in assisting others in sanctions violations is separate from OFAC?s well known doctrine of ?facilitation? by U.S. persons in assisting foreign parties in sanctions violations.

[17] The theories of jurisdiction under which foreign companies can be subject to U.S. sanctions has been increasing based upon a growing number of recent OFAC enforcement cases against foreign companies.

[18] See additional discussion of prohibited facilitation in section C.7 below.

[19] The scope of these general licenses may very under certain of the sanctions programs.

[20] Most sanctions programs are initiated by the President issuing an Executive Order declaring a national emergency under IEEPA and the National Emergencies Act and designating parties who will be the target of the sanction. OFAC will then frequently issue regulations and begin licensing activities related to the program. However sanctions programs have also been mandated by Congress under specific legislation, either to initiate a sanctions program (such as in the Venezuela program) or to amend it later on (such as amendments to the Iran, N. Korea and Russia programs under the Countering America?s Adversaries Through Sanctions Act (?CAATSA?). They may also be adopted in response to United Nations resolutions or other multilateral obligations. Once initiated, the programs are frequently amended through subsequent Executive Orders, regulations and statutory mandates ? for example under the Iran sanctions program there are 11 separate statutes, 27 executive orders and 4 complete sets of regulations. While the sanctions programs are typically driven the by the Executive Branch, in certain cases Congress can be the driving force, often for political reasons. For example, under the recently enacted CAATSA Congress has imposed requirements that President Trump adopt additional sanctions on Iran, Russia and North Korea, and that prohibit the repeal of certain Russian sanctions by the President without Congressional authorization.

[21] There are no open judicial proceedings required for a party to be designated on the SDN List. Rather determinations are made by the Treasury Department in conjunction with the State Department and other federal agencies in a non-public process. While designated parties are permitted to challenge the designation through a submission to OFAC, this process does not provide for procedural protections such as the right to the cross-examination of witnesses, etc.

[22] Penalties for violations include civil and criminal penalties. Criminal penalties are up to twenty years imprisonment, $1,000,000

in financial fines, or both per violation. Civil penalties are up to the greater of $307,922 or twice the amount of the underlying transaction, per violation subject to adjustment under the Federal Civil Penalties Adjustment Act. OFAC has a robust enforcement division which initiates civil enforcement cases. In addition, the U.S. Justice Department in Washington, D.C. and individual U.S. Attorneys? offices initiate criminal prosecutions of sanctions violations, sometimes in conjunction with OFAC or independent of the agency. Judicial review of OFAC determinations is authorized under most of the sanctions programs, but cases are limited. (See, eg., Epsilon Electronics Inc. v. U.S. Dept. of the Treasury Office of Foreign Assets Control, Et. Al., In the U.S. Court of Appeals for the District of Columbia Circuit, No. 16-5118, May 26, 2017.).

[23] For example, under the EAR the Bureau of Industry and Security regulates transactions with many of the countries subject to OFAC sanctions under 15 CFR Part 746 (Embargoes) including Iran, Syria, Russia, Cuba, Iraq, N. Korea, Iran and Crimea. Similarly the EAR sets forth restrictions on transactions with Russia that are separate from the OFAC Russia requirements, including the Russian Industry Sector Sanctions set forth at 15 CFR §746.5, restrictions on dealings with certain Russian parties under 15 CFR §744.10 and restrictions on dealing with military end use and military end users in Russia under 15 CFR §744.21. In addition, as referenced above, the President may be mandated to impose additional Russian sanctions in the future under CAATSA. Further, BIS maintains three restricted party lists which must be reviewed in addition to the OFAC restricted party lists (which include many Russian individuals and entities). The recent enforcement case involving ZTE Corp. was initiated jointly by BIS and OFAC for violations of the EAR and OFAC sanctions.

[24] See e.g., 31 CFR §501.601.

[25] See e.g., 31 CFR §501.603.

[26] See OFAC Guidance document: ?Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,? October 1, 2020, available on OFAC?s website.

[27] Issued on October 30, 2020; available on OFAC?s website.

[28] The BIS Russia Industry Sector Sanctions are set out at 15 CFR §746.5 and the OFAC Russian sectoral sanctions are set forth in Executive Order 13662 and the Directives promulgated thereunder.

[29] See 15 CFR §746.5(a)(1).

[30] Transactions with Russian financial institutions under the OFAC Russia sectoral sanctions for the Russian financial sector under Executive Order 13662 and related Directives may also prohibit related financial transactions in certain instances ? See OFAC Frequently Asked Questions No. 395.

[31] See OFAC Guidance document: ?Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,? October 1, 2020, available on OFAC?s website.

[32] See OFAC Guidance document: ?Advisory and Guidance on Potential Sanctions Risks Arising from Dealings in High-Value Artwork,? October 30, 2020, available on OFAC?s website.

[33] See OFAC release ?Revised Guidance On Entities Owned By Persons Whose Property and Interests In Property Are Blocked,? August 13, 2014, available on OFAC website.

[34] Under OFAC guidance, ?Reason to know? that the seller?s goods are intended for Iran can be established through a variety of

circumstantial evidence, such as: course of dealing, general knowledge of the industry or customer preferences, working relationships between the parties, or other criteria far too numerous to enumerate . . . .? See OFAC guidance document: ?Guidance On Transshipments to Iran? available on the OFAC website.

[35] In one recent case a U.S. company was found to have violations for reexports to Iran when it failed to identify information on the foreign customer?s website that the foreign customer engaged in business transactions with Iran. See Epsilon Electronics, Inc. v. United States Department of the Treasury, Office of Foreign Assets Control, et al., Civil Action No. 14-2220 (RBW), In the U.S. District Court For the District of Columbia.

[36] Even for country-based programs in which the U.S. company?s foreign subsidiaries are permitted to engage in transactions with countries subject to comprehensive sanctions, however, the U.S. parent company and its U.S. employees are strictly prohibited from having any involvement in such transactions including through assisting, approving, providing products/components, technology, funding, and management support for such transactions. See Section C.7 below.

[37] Such instances may include where such activities are permitted under the specific sanctions program or in some cases where activities are authorized under specific or general license.

[38] See for example OFAC guidance ?Crimea Advisory - Obfuscation of Critical Information in Financial and Trade Transactions Involving the Crimea Region of Ukraine,? July 30, 2015, available on OFAC website.

[39] See OFAC announcement of enforcement settlement at: https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20150325_33.

Related People

- Christopher H. Skinner ? 202.293.8129 ? cskinner@williamsmullen.com

Related Services

- International Trade and Business
- ITAR, Export Controls and Economic Sanctions