2016 CLM Annual Conference
April 6-8, 2016
Orlando, FL

"Avoiding High Stakes Penalties and Loss of Government Contracts"

1. Who, What, How: Office of Foreign Asset Control (OFAC), Bureau of Industry & Security (BIS) and United States Department of State (DOS)

a. Office of Foreign Asset Control

The Office of Foreign Assets Control ("OFAC") is a financial intelligence and enforcement agency of the US Department of the Treasury, tasked to administer and enforce economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the U.S. economy, security, and foreign policy. OFAC acts under the Trading with the Enemy Act (1917), International Emergency Economic Powers Act (1977), Presidential national emergency powers and specific legislation to restrict certain transactions, freeze assets under U.S. jurisdiction, and impose sanctions. Many of the sanctions are based on United Nations and other international mandates, are multilateral in scope, and involve close cooperation with allied governments.

OFAC sanctions have a strict liability component, which means liability is imposed for violations of the law regardless of the fault or criminal intent of the individual.

OFAC's defines prohibited transactions as following: "Trade or financial transactions and other dealings in which U.S. persons may not engage unless authorized by OFAC or expressly exempted by statute. Because each program is based on different foreign policy and national security goals, prohibitions may vary between programs."[1]

Who is subject to those regulations? All U.S. citizens and permanent resident aliens regardless where they are located, all persons physically in the U.S. regardless of their citizenship must comply with OFAC sanctions. In addition, U.S. entities, all branches of U.S. entities throughout the world and U.S. branches or offices of foreign corporations physically located in the U.S. are also subject to OFAC sanctions. In the cases of certain programs, foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S.-origin goods to comply

There are three Specific Economic Sanctions categories:

- Comprehensive Sanctions - contain restrictions that are triggered merely because an entity is conducting a transaction in, with a person from, or with the government of a specific country. These countries are the Crimea Region of Ukraine, Cuba, Iran, Sudan and Syria.

[1] https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_general.aspx#basic

- Limited Sanctions - they differ from comprehensive sanctions in that limited sanctions are typically less restrictive and are applied to only certain transactions. These countries include Burma (aka Myanmar), Libya and North Korea.
- List-Based Sanctions - while many countries are subject to economic sanctions, some of these sanctions are merely sanctions which result in names being added to the OFAC Sanctions Lists. These countries are The Balkans (consisting of Bosnia, Herzegovina, Kosovo, Macedonia and Montenegro), Belarus, Côte d'Ivoire (Ivory Coast), Central African Republic, Democratic Republic of the Congo, Iraq, Lebanon, Former Liberian Regime of Charles Taylor, Russia, Somalia, South Sudan, Ukraine, Venezuela, Yemen and Zimbabwe. Because of their flexibility, list based sanctions are now the standard for OFAC sanctions programs. List-based sanctions have become the norm for law enforcement-based economic sanctions programs. An example of the implementation of list-based sanctions can be found in President Barack Obama's Executive Orders which use list-based sanctions for the Ukraine-Related Sanctions Program.

Other prohibited actions:

- Use of some foreign flag vessels or airlines (Cuban-, Iranian-, Sudanese- and Syrian-flag). For example, during your vetting process, a vessel's name is not found within the SDN list, however because the vessel flies the flag of one of above mentioned countries, using the vessel is a prohibited transaction. OFAC places a different set of restrictions on North Korean flagged vessels.
- Through Transit or Transshipment Provision: the shipment of freight by ocean, air or land which travels through the countries of Cuba, Crimea region of Ukraine, Iran or Sudan is prohibited. Let's say you have a shipment originating in Afghanistan bound for Turkey, the most direct route is by ground via truck through Iran to Kurdistan and then to Turkey. However, because Iran has comprehensive sanctions (one is not allowed to "enter" Iran) the shipment must be routed differently.
- Facilitation Provision: facilitation occurs when a U.S. Party subject to OFAC sanctions aids a transaction they are prohibited from conducting themselves. Facilitation includes referring the business to a third party, moving goods to an intermediate country if the shipment's ultimate destination is prohibited, shipping to an intermediary if the end user is a party on the SDN list, or in any way participating in, or providing assistance with, a prohibited transaction.

b. The Bureau of Industry & Security

The Bureau of Industry & Security's ("BIS") mission is to: "Advance U.S. national security, foreign policy, and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership."[2]

The main body of law administered by BIS is the Export Administration Regulations ("EAR"). Under the EAR, all goods exported from the U.S. must be licensed, unless no license is required for that item. EAR also applies to the following:

- Goods of foreign origin located in the U.S. being exported out of the U.S.
- Foreign-made products incorporating U.S. content
- Foreign-produced direct products of U.S. technology or software
- Any "re-exports" of U.S. origin items from anywhere in the world

The "deemed export" rule is an export of technology or source code (except encryption source code) which is "deemed" to take place when it is released to a foreign national within the United States[3].

[2] http://www.bis.doc.gov/index.php/about-bis/mission-statement
[3] See §734.2(b)(2)(ii) of the Export Administration Regulations (EAR)

EAR defines "technology" as specific information necessary for the "development," "production," or "use" of a product. The General Technology Note states that the "export of technology" is controlled according to the provisions of each Category." It further states that "technology required for the development, production, or use of a controlled product remains controlled even when applicable to a product controlled at a lower level.[4]

Special consideration should be granted to dual-use items, which are items having both a civilian and military use. The Bureau will strongly administer and enforce the rules in order to stem the proliferation of weapons of mass destruction, the means of delivering them, and halt the spread of weapons to terrorists or countries of concern, as well as to further important U.S. foreign policy objectives. For example, a dip-stick used to measure oil. If the item is for a regular car, it may not require a license to export (depending on the destination country), however the same dip-stick specifically make for a military tank will more than likely require a license.

The Commerce Controlled List ("CCL") is a list of items including but not limited to dual use items (example), commodities, software and technology which are subject to exporting regulations by BIS. The CCL is divided as following[5]:

Commerce Control List Categories	
0	Nuclear & Miscellaneous
1	Materials, Chemicals, Microorganisms and Toxins
2	Materials Processing
3	Electronics
4	Computers
5 Part 1	Telecommunications
5 Part 2	Information Security
6	Sensors and Lasers
7	Navigation and Avionics
8	Marine
9	Aerospace and Propulsion

Five Product Groups	
A	Systems, Equipment and Components
B	Test, Inspection and Production Equipment
C	Material
D	Software
E	Technology

BIS is also charged with administering and enforcing the Antiboycott Laws under the Export Administration Act which applies to all boycotts by foreign countries unsanctioned by the U.S. Those laws discourage, and in some circumstances, prohibit U.S. companies from furthering or supporting the boycott of Israel sponsored by the Arab League for example, and certain other countries, including complying with certain requests for information designed to verify compliance with the boycott. Compliance with such requests may be prohibited by the Export Administration Regulations (EAR) and possibly reportable to the Bureau.

U.S. antiboycotting laws and regulations are designed to deter cooperation with international economic boycotts in which the U.S. does not participate. EAR's antiboycott provisions apply to the activities of U.S. persons in U.S. interstate or foreign commerce. The term "U.S. person" includes all individuals, corporations and unincorporated associations resident in the United States, including the permanent domestic affiliates of

[4] Part 772 of the Export Administration Regulations (EAR)
[5] http://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

foreign concerns. U.S. persons also include U.S. citizens abroad (except when they reside abroad and are employed by non-U.S. persons) and the controlled in fact affiliates of domestic concerns. The test for "controlled in fact" is the ability to establish the general policies or to control the day to day operations of the foreign affiliate."[6]

Those provisions prohibit agreements to refuse or actual refusal to do business with or in Israel or with black listed companies; agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality; agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies, about the race, religion, sex, or national origin of another person.

c. United States Department of State (DOS)

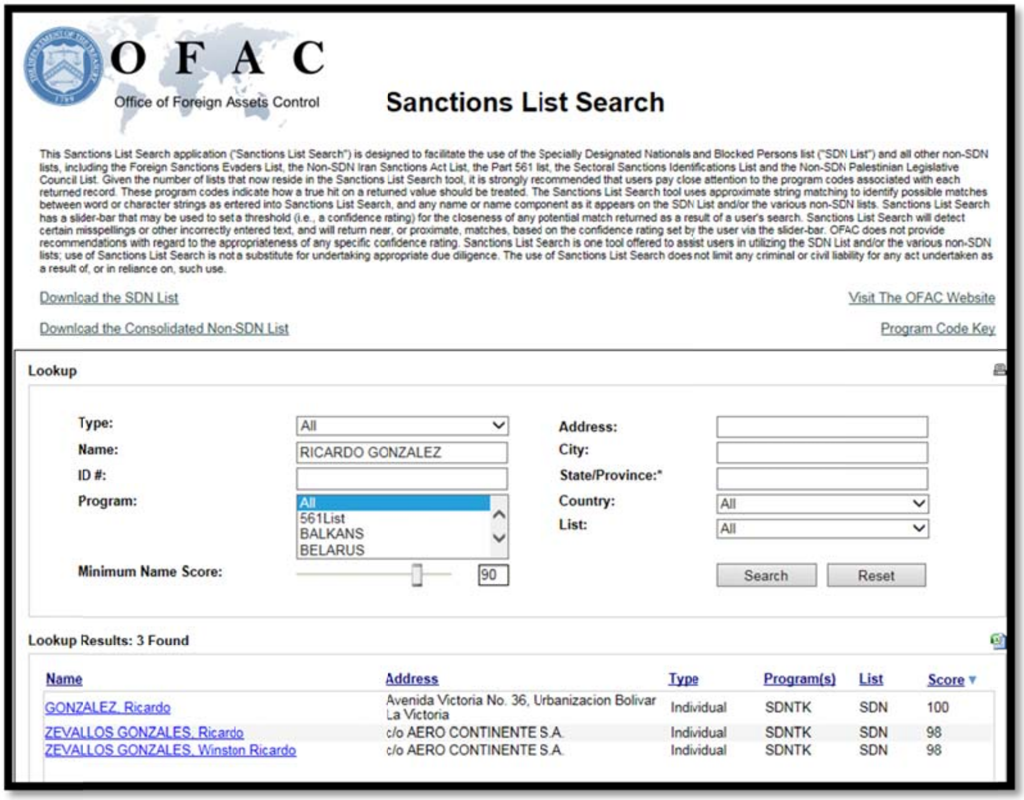
The Department of State's Directorate of Defense Trade Controls (DDTC), is responsible for the international relations of the United States, equivalent to the foreign ministry of other countries, as well as for the export and temporary import of defense articles and services.[7] The International Traffic In Arms Regulations (ITAR) is another set of regulations companies should be mindful of because it also presents pitfalls for the unwary. For example, a company that uses remotely operated underwater vehicles could run into problems with ITAR if it does business worldwide and imports and/or exports its equipment to and from the U.S. without a license from the Department of State because the remotely controlled vehicle ("ROV") has a global positioning device which is extremely accurate and could be removed from the ROV and used to guide torpedoes, bombs, etc. Further discussion of ITAR is beyond the scope of the panel's presentation.

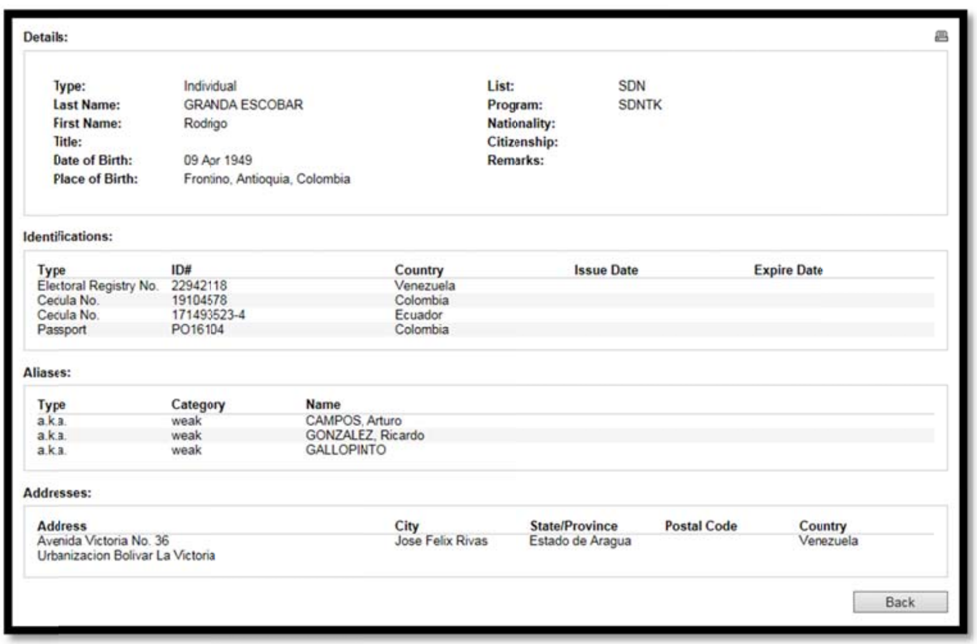
d. Specially Designated Nationals List ("SDN") & Consolidated Sanctions List

Parties on these lists include terrorists, sponsors of terrorist activity and terrorist organizations, narcotics traffickers and kingpins, agents of sanctioned country governments and proliferators of weapons of mass destruction. The Sanctions Lists is not static and currently contains thousands of entries, which include not just names but other known information (e.g., aliases, date of birth, last known residential or business address, passport number, web sites, etc.). For example, Joaquin Guzman Loera (El Chapo), the drug kingpin that was recently captured, was born on Christmas day 1954 and has 18 different aliases. Below is another example of the information available on the Sanctions List which is accessible by computer.

[6] http://www.bis.doc.gov/index.php/enforcement/oac

[7] Governed by 22 U.S.C. 2778 of the Arms Export Control Act ("AECA"; see the AECA Web page) and Executive Order 13637. The International Traffic in Arms Regulations ("ITAR," 22 CFR 120-130) implements the AECA.





There is a complete prohibition in doing business of any kind with individuals or entities on the Sanctions lists, unless a license has been issued by the appropriate regulating body.

e. Exceptions, Exemptions and Licenses

- OFAC regulations often provide general licenses authorizing the performance of certain categories of transactions. OFAC also issues specific licenses on a case-by-case basis under certain limited situations and conditions. The specific licenses are issued to a particular person or entity, authorizing a particular transaction in response to a written license application.[8]

- BIS – The Bureau receives submission of export and re-export license applications, commodity classification requests, license exception notifications via its online *Simplified Network Application Process–Revised* (SNAP-R) platform.

There is frequently more to consider than obtaining a license to export or to provide specific services under a license. Another critical consideration is methods payment for the licensed services and payments to vendors. Financial institutions are held to numerous laws and regulations, and may not want to risk potential fines, etc. related to the transaction, even if you have been granted a license, or the general license was issued for the specific area or specific industry/services.

2. Enforcement, Penalties & Exposures

a. Enforcement & Penalties

Dealings with any parties on the SDN List or Consolidated Sanctions Lists may be criminally or civilly penalized regardless whether the transaction involves a sanctioned or non-sanctioned country.

- **Office of Foreign Asset Control**
  The fines for violations can be substantial. Depending on the program, criminal penalties for willful violations can include fines ranging up to $20 million and imprisonment of up to 30 years. Civil penalties for violations of the Trading With the Enemy Act can range up to $65,000 for each violation. Civil penalties for violations of the International Emergency Economic Powers Act can range up to $250,000 or twice the amount of the underlying transaction for each violation. Civil penalties for violations of the Foreign Narcotics Kingpin Designation Act can range up to $1,075,000 for each violation.

- **Bureau of Industry & Security Penalties**
  Violations of the Export Administration Act of 1979, as amended (EAA), 50 U.S.C. app. §§ 2401-2420 (2000), and the Export Administration Regulations, 15 C.F.R. Parts 730-774 (2007) (EAR) may be subject to both criminal and administrative penalties. When the EAA is in effect, criminal penalties can reach 20 years imprisonment and $1 million per violation. Administrative monetary penalties can reach $11,000 per violation, and $120,000 per violation in cases involving items controlled for national security reasons. When the EAA is in lapse, the criminal and administrative penalties are set forth in the International Emergency Economic Powers Act (IEEPA).
  BIS – 2014 assessed the following:
    - Criminal penalties: 39 individuals and business convicted, $137,808,756 in criminal fines, $1,318,832 in forfeitures, 568 months of imprisonment
    - Administrative penalties: 44 administrative cases, $60,488,000 in administrative penalties

  The Export Administration Act (EAA) specifies penalties for violations of the Antiboycott Regulations as well as export control violations. These can include:
    - Criminal: The penalties imposed for each "knowing" violation can be a fine of up to $50,000 or five times the value of the exports involved, whichever is greater, and imprisonment of up to five years. During periods when the EAR are continued in effect by an Executive Order issued pursuant to the International Emergency Economic Powers Act, the criminal penalties for each "willful" violation can be a fine of up to $50,000 and imprisonment for up to ten years.
    - Administrative: For each violation of the EAR any or all of the following may be imposed:

[8] Guidance on how to request a specific license can be found under 31 C.F.R. 501.801.

- General denial of export privileges;
- The imposition of fines of up to $11,000 per violation; and/or
- Exclusion from practice.

When the EAA is in lapse, penalties for violation of the Antiboycott Regulations are governed by the International Emergency Economic Powers Act (IEEPA). The IEEPA Enhancement Act provides for penalties of up to the greater of $250,000 per violation or twice the value of the transaction for administrative violations of Antiboycott Regulations, and up to $1 million and 20 years imprisonment per violation for criminal antiboycott violations.[9]

- **Beyond the Regulatory Agencies Fines & Penalties**
  Not only can a company be fined, lose exporting privileges (and perhaps in worst case scenario be imprisoned), those penalties could potential cause the company to be prevented from bidding on government contracts or even worst, lose every government contract they currently hold. Beyond the loss of government contracts, the company can be viewed as reckless and too high of an exposure risk, prompting clients seek another partner.

b. Domestic Exposures

- Party on the consolidated sanctions list
- Ultimate user
- Facilitation
- Export or re-export without proper license

c. International Exposures

- Party on the consolidated sanctions list
- Ultimate user and/or destination
- Facilitation
- Trans-shipment or Through Transit
- Export or re-export without proper license
- Antiboycott
- Location of the transaction
- Supply Chain & vendors

d. Internal Exposures

- No buy-in/support from the C-Suite
- Ignorance of laws and regulations; not keeping up with fluid changes in the laws and regulations
- Lack of compliance policies
- Not enforcing the company compliance policies
- Lack or no employee training

e. Example: Cuban nationals located in Florida (case study). Main transferee works for a Fortune 500 company, the employer is paying for the relocation from Florida to the Midwest. Co-transferee, the significant other, is not a green card holder and has not yet applied for a change in status. The moving company advised the client it could not provide services for this relocation

[9] http://www.bis.doc.gov/index.php/enforcement/oac

based on the fact the relocation was above what would be considered as usual maintenance (i.e. groceries, bus, doctor's visit) for a Cuban national before the change of status or the application for the change of status as was the case for the co-transferee. The request to only move the main transferee's effect only was also denied, as the moving company could not ascertain with certainty only the main transferee's items would be packed and moved. One last argument made was to remove the name of the co-transferee from the order and paperwork in order to proceed with the move, which was also denied by the moving company. Had the moving company removed the co-transferee's name from the order/paperwork and proceeded with the move, both the moving company and the client could have been held liable by the Department of Treasury, as they knowingly 1) facilitated a prohibited transaction and 2) altered the paperwork, potentially exposing themselves to a willful misconduct fines.

3. Prevention & Mitigation

a. Prevention

- Risk Assessment: identify your exposure. Line of business, geographical locations of foreign branches, business target area, supply chain, partners & customers profiles. Due diligence. New risk assessment if significant changes happen within the company or outside the company's control. Periodical review of the compliance program (annual, bi-annual, etc…) and make appropriate changes when necessary.
- Compliance program: secure C-suite support, draft a policy, define key roles with the appropriate authority to take action if warranted (this should include outside counsel) within the compliance team, training (initial & ongoing), accountability and disciplinary actions. What list(s) will you scan against? In-house screens against the chosen lists or do you enlist the help of a third party? What data will be screened (name only, addresses, etc…)? Potential List match & Positive List match procedures. How is the sensitive data going to be protected? Who will handle the contact with the authorities and administrative subpoenas?
- Supply Chain, Partners & Vendors: due diligence, screening, vetting and educating. Contract language and indemnification agreements. Mutual confidential agreements.
- Clients: due diligence, screening vetting and educating. Contract language and indemnification agreements. Mutual confidential agreements.
- Transaction specific: does it require an export or re-export license? Who are the parties to the transaction? Geographical location?
- Geographical area: is the country or region have any restrictions or sanctions?
- Mergers & Acquisitions: what exposures are we potentially taking on?
- Record keeping: documentation, documentation, documentation! Compliance policies, training, licenses, actions related to specific transactions (why we did what we did).

b. Mitigation

- Voluntary Self-Disclosure
- Indemnification agreements with third parties
- Corrective training & disciplinary actions
- Record keeping