# DOS AND DON'TS FOR COMPLIANCE PERSONNEL AT INTERNATIONAL NON-PROFITS

17th Annual Compliance & Ethics Institute

October 23, 2018

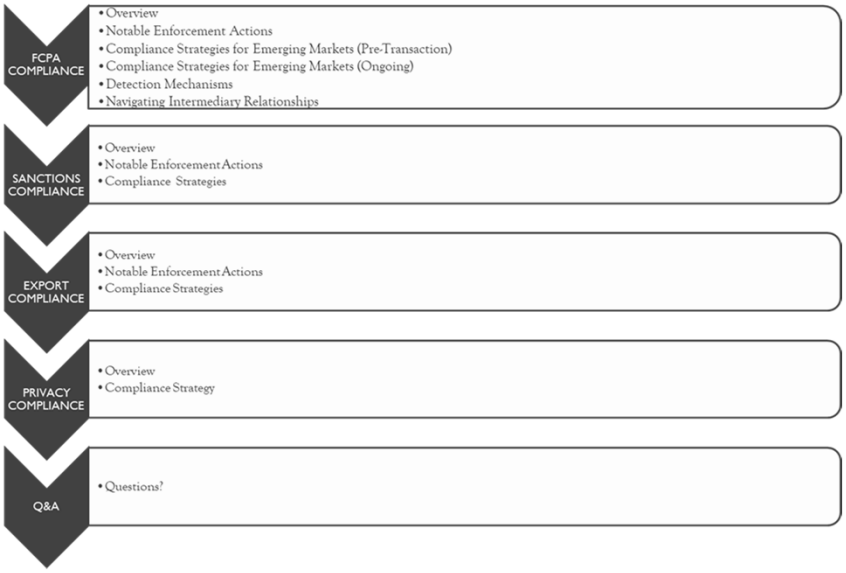
**Adam Munitz**
FH+H, PLLC
Global
amunitz@fhhfirm.com

**Hussainatu Blake**
Focal Point
hussablake@gmail.com

## KEY CHALLENGES FACING NON-PROFITS WORKING INTERNATIONALLY

- Ineffective controls for corruption
- Limited financial controls
- Failing to meet funding partner expectations
- Losing control of intellectual property

# ROADMAP




# FOREIGN CORRUPT PRACTICES ACT COMPLIANCE

# OVERVIEW

## WHAT IS THE FCPA?

The FCPA is an U.S. law prohibiting payments to foreign officials in exchange for preferential treatment.

## WHAT CONSTITUTES A "FOREIGN OFFICIAL?"

- FCPA prohibits corrupt payments to:
  - Any government official of a department, agency, or instrumentality, of the US government, or public international organization, or foreign political party or foreign state-owned or state-controlled entity.
- BUT WAIT: In addition, corrupt payments to an otherwise permitted individual may also be prohibited if the payer *knows* that such individual will, in turn, offer, give, or promise the payment (or part of the payment) to a foreign official.
- How do I know if I "know?"
  - If you actually know that the ultimate recipient of the payment is a foreign official;
  - If you avoid knowing that the ultimate recipient of the payment is a foreign official; or
  - If you ignore signs that the ultimate recipient of the payment is a foreign official.

## WHAT CONSTITUTES A "CORRUPT PAYMENT?"

- Anything of value!
  - Travel Expenses
  - Gifts
  - Entertainment
  - CASH
- Success & Magnitude = Irrelevant
  - Mere offering constitutes a violation
  - Even idiosyncratic gifts lacking value constitute a corrupt payment
- "Corrupt" Payment = it must be made with the intent to incentivize the recipient to abuse his/her authority by granting preferential treatment, failing to take action, or improperly directing business towards the payer.
- **NOTE:** U.S.-based nonprofit or association can be held liable for the acts of partners abroad under FCPA

## FOREIGN CORRUPT PRACTICES ACT (FCPA)

# NOTABLE ENFORCEMENT ACTIONS

## NOTABLE ENFORCEMENT ACTIONS

1. Pitchford (2011)
   - Pitchford, a former employee of the Central Asian American Enterprise Fund, which was formed and wholly-funded by Congress, arranged for purchases of equipment at inflated prices and obtained confidential bid information in exchange for kickbacks.
   - Total criminal and regulatory penalties: **12 months in prison, 3 years supervised release, and $400,000 in restitution.**
2. Novak (2011)
   - Novak, an employee of two individuals that operated online "universities," bribed Liberian officials in exchange for university accreditations.
   - Total criminal and regulatory penalties: **3 years probation.**

## FOREIGN CORRUPT PRACTICES ACT (FCPA)

# COMPLIANCE STRATEGIES

## FCPA COMPLIANCE STRATEGIES FOR EMERGING MARKETS- PRE-TRANSACTION COMPLIANCE STRATEGIES

1. **Legal, regulatory and cultural research**
   - Identify controlling entities
     - Government?
     - Military?
     - Militias/Tribes?
   - Local presence requirements
     - Likely in flux, so distinguish formal from informal requirements
   - Permit requirements (if any)
     - Business licenses
     - Visas
     - Customs permits
   - Cultural pressure points
   - Transparency International
   - Leverage in-country network
2. **Identify and assess all intermediaries pre-transaction**
   - Local representatives
   - Consultants
   - Logisticians
   - Close-protection security
   - Couriers
   - Transportation providers
   - Translators
3. **Set Tone**
   - Establish low tolerance for corruption at outset

## FCPA COMPLIANCE STRATEGIES FOR EMERGING MARKETS- ONGOING COMPLIANCE STRATEGIES

1. **Experienced cadre of in-country support staff**
   - Lawyers
   - Business people
   - Community Leaders
2. **In-country situational awareness**
   - Scheduled and unscheduled visits to intermediaries, support personnel, and clients
   - Communicate, communicate, communicate!
3. **Sophisticated reporting requirements and mechanisms**
   - Internal
   - External
4. **Hyper-focused accounting personnel**
   - Remember- the first signs of corruption will appear in irregular financial reporting
5. **Alertness to political, legal, regulatory, military, and religious shifts**
6. **Adaptability**
   - Continually assess and re-assess efficacy of compliance strategy in light of in-country events and evolving client requirements
7. **Dynamic disclosure strategy**
8. **Ongoing communications with trade counsel**

# NAVIGATING INTERMEDIARY RELATIONSHIPS

1. **Thorough Due Diligence**
   - Initiate Early
   - International Party Questionnaires
   - Anti-Corruption Certifications
   - Investigative Follow-Up
   - Red Flags
2. **Effective Training**
   - Practical Approach
   - In-Person
   - Training Modules
     - Assess responses!
   - Emphasize:
     - Consequences (legally and contractually)
3. **Sustained Monitoring**
   - Robust Accounting Program
   - Frequent and In-Person Contact

# CASE STUDY: PROGRAMS SPONSORED BY FOREIGN GOVERNMENTS

UNIVERSITY OF THE WITWATERSRAND JOHANNESBURG

FORDFOUNDATION

EXPORT COMPLIANCE

# OVERVIEW

## WHAT IS EXPORT COMPLIANCE?

A critical component of the U.S. national security strategy is the organized control of goods and services that, in the wrong hands, would harm our national security interests or frustrate our international objectives/priorities.

Accordingly, the U.S. government has passed laws, and implemented regulations, that limit the ability of U.S. persons to export defense articles, defense services, dual-use items, technical assistance, and controlled technical data without prior governmental approval.

The export compliance regulations on which we will be focused today are the International Traffic in Arms Regulations and the Export Administration Regulations.

# PENALTIES

- ITAR
  - Criminal Penalties
    - ➢ Willful violations, misrepresentations, or omissions can result in criminal fines of up to **$1,000,000** and/or up to **20 years** imprisonment per violation.
  - Civil Penalties
    - ➢ Depending on the nature of the violation, individuals and entities can be fined anywhere from **$824,959** per violation to **$1,134,602** per violation.
  - Administrative Debarment (typically 3 years)

- EAR
  - Criminal Penalties: Up to **$1,000,000** and/or **20 years** imprisonment per violation.
  - Administrative Penalties: The greater of **$250,000** per violation or **twice the amount of the transaction** that is the basis of the violation.
  - Administrative Debarment

# WHAT IS THE ITAR?

- The International Traffic in Arms Regulations ("ITAR") are U.S. regulations that control the temporary and permanent export, and temporary import, of "defense articles" (e.g., military equipment), technical data related to defense articles, and defense-related services.

- The ITAR prohibits the temporary and permanent export of defense articles, technical data, and defense services from the U.S. abroad or to a foreign person/entity, unless the export is authorized by the Directorate of Defense Trade Controls ("DDTC") at the U.S. Department of State or an ITAR exemption applies.

# ITAR: KEY TERMS

- Defense article: any item that is described in the United States Munitions List, 22 C.F.R. § 121.1 (the "USML"), or provides the equivalent performance capabilities of an item described in the USML.
- Technical data: information recorded or stored in any physical form, models, mockups, or other items that reveal technical data relating to items described in the USML.
- Defense service: any one of the following:
  - ➢ Furnishing assistance (including training) to foreign persons, either in the United States or abroad, in the design, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing or use of defense articles;
  - ➢ Furnishing ANY technical data to ANY foreign person, either in the United States or abroad; or
  - ➢ Military training of foreign units and forces, regular and irregular, including formal or informal instruction of foreign persons in the United States or abroad or by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation, training exercise, and military advice.

# WHO IS SUBJECT TO THE ITAR?

- U.S. persons (i.e., lawful permanent resident, asylee, or refugee OR business entity incorporated/organized in the U.S.) must obtain DDTC authorizations to export or temporarily import items and services regulated by the ITAR.
- U.S. persons, and foreign persons located in the United States or located outside of the United States but owned or controlled by a U.S. person, must obtain DDTC authorizations to broker the sale of items and services regulated by the ITAR.
- The following U.S. persons are ineligible for DDTC authorization:
  - ➢ Anyone convicted of violating specific criminal statutes;
  - ➢ Anyone debarred from contracting with the U.S. government;
  - ➢ Anyone ineligible to receive an export authorization from any other U.S. government agency; and
  - ➢ Anyone whose export license has been suspended or revoked.

# WHAT IS THE EAR?

- The Export Administration Regulations ("EAR") are U.S. regulations that control the export of "dual-use" items (i.e., articles that have both a military and a commercial application) and information related to such items ("Technology").

- The EAR prohibits the temporary and permanent export of certain dual-use items and "Technology" from the United States to certain countries and certain foreign nationals, unless the export is authorized by the Bureau of Industry and Security ("BIS") at the U.S. Department of Commerce, or an EAR exemption applies.

# WHICH DUAL-USE ITEMS ARE REGULATED?

- The EAR regulates those commercial and dual-use items found on the Commerce Control List ("CCL" "CCL").
- The CCL consists of 10 categories:

  0. Nuclear Materials, Facilities, and Equipment (and Miscellaneous Items)
  1. Special Materials and Related Equipment, Chemicals, and Microorganisms, and Toxins
  2. Materials Processing
  3. Electronics
  4. Computers
  5. Telecommunications and Information Security
  6. Sensors and Lasers
  7. Navigation and Avionics
  8. Marine
  9. Aerospace and Propulsion

- These categories are, in turn, further divided into five product groups:
  A. Systems, Equipment, and Components
  B. Test, Inspection, and Production Equipment
  C. Material
  D. Software
  E. Technology

- NOTE: Even if your export is not included on the CCL it may still require a license if, for example, it is destined for a *prohibited party* (*see* EAR Part 744).

## WHAT CONSTITUTES "TECHNOLOGY" UNDER THE EAR?

- Under the EAR, technical information relating to controlled dual-use items AND the communication of such technical information are both characterized as "Technology."

  - "Technology" is defined in EAR Part 772 as "[i]nformation necessary for the "development," "production," "use," operation, installation, maintenance, repair, overhaul, or refurbishing (or other terms specified in ECCNs on the CCL that control "technology") of an item.

    - NOTE 1: "Technology" may be in any tangible or intangible form, such as written or oral communications, blueprints, drawings, photographs, plans, diagrams, models, formulae, tables, engineering designs and specifications, computer-aided design files, manuals or documentation, electronic media or information revealed through visual inspection[.]"

- Accordingly, the provision of training and instruction in which technical information is communicated to a foreign person is regulated under the EAR as "Technology," just as the provision of training and instruction during which technical data pertaining to defense articles is communicated to foreign persons is regulated as a "defense service" under the ITAR.

## THE EAR99 DESIGNATION

- If an item falls under the jurisdiction of BIS but is not listed on the CCL, then it is designated as "EAR99."
- Before exporting an EAR99 item (i) to an embargoed or sanctioned country; (ii) to a party of concern; or (iii) in support of a prohibited end use, an exporter may be required to obtain a license.

## HOW DO I KNOW IF I AM "EXPORTING" IN THE FIRST PLACE?

- **ITAR**
  - An actual shipment or transmission out of the United States, including the sending or taking of a defense article out of the United States in any manner;
  - Transferring registration, control, or ownership of any aircraft, vessel, or satellite subject to the ITAR by a U.S. person to a foreign person;
  - Releasing or otherwise transferring a defense article to an embassy or to any of its agencies or subdivisions, such as a diplomatic mission or consulate, in the United States;
  - Performing a defense service on behalf of, or for the benefit of, a foreign person, whether in the United States or abroad; or
  - Releasing technical data in the United States to a foreign person (i.e., a "**deemed export**" to the countries in which the foreign person has held or holds citizenship or holds permanent residency).
    - Visual or other inspection by foreign persons of a defense article that reveals technical data to a foreign person; or
    - Oral or written exchanges with foreign persons of technical data in the United States or abroad.
- **EAR**
  - 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" or source code (but not object code) to a foreign person in the United States (a "**deemed export**");
  - Transferring by a person in the United States of registration, control, or ownership of:
    - A spacecraft subject to the EAR that is not eligible for export under License Exception STA...; or
    - Any other spacecraft subject to the EAR to a person in or a national of a Country Group D:5 country.

## WHO QUALIFIES AS A FOREIGN PERSON?

- Any natural person not a lawful resident or "protected individual" under 8 U.S.C. § 1324(a)(3) (i.e., a person lawfully admitted into the United States as an asylee or refugee);
  - NOTE: VISA HOLDERS ARE NOT U.S. PERSONS!
- Any foreign corporation, business association, partnership, or other entity not incorporated/organized to do business in the United States;
- Any international organization, such as the United Nations; and
- Foreign governments and any agency or subdivision thereof (e.g., diplomatic missions).

## COMPLYING WITH THE ITAR AND THE EAR- EXPORT LICENSES AND EXEMPTIONS/EXCEPTIONS

- Generally speaking, unless an exclusion or an exemption applies, a U.S. person MUST obtain an export authorization from the U.S. government before exporting any defense articles, CCL-controlled items, technical data, defense services, or technology. This authorization comes in the form of a "license."
- NOTE: Under the EAR, the precise destination of an export will invariably determine whether a license is required.

## COMPLIANCE STRATEGIES

The ITAR and the EAR are highly-complex regulations, and complying with such regulations is no easy task. There are two strategies that exporters can implement, however, to consistently export in a lawful manner. The first is to conduct thorough due diligence in advance of every export, and the second is to develop an effective export compliance program.

# DUE DILIGENCE

- Objective: To determine whether a license issued by DDTC or BIS is required for the transaction, or whether an exemption to the licensing requirement applies.
- The "What"
  - Determine the types of goods and/or services being exported, and their components, and whether they are covered by the ITAR, the EAR, or neither regulation.
  - Determine whether goods being exported contain any *components* that will be covered by U.S. export controls.
    - ➢ Taking the foregoing measures will help define the sub-agency with which exporters must liaise (DDTC or BIS) in order to secure export licenses.
- The "Who"
  - Determine the specific recipients and end users of the goods, services or information.
  - In what countries are such recipients and end users residents (if individuals) or organized (if companies or organizations)?
  - Are there any parent entities? What are the nationalities of the shareholders?
    - ➢ Asking these questions will (a) provide the requisite information for a license application; and (b) help determine whether the end users are proscribed parties under the Specially Designated Nationals List, the Denied Persons List, the Entities List, those countries listed at ITAR § 126.1, or the BIS' List of Parties of Concern.
- The "Where"
  - Probably synonymous with the nationality of the end user, but goods delivered abroad often transit a number of intermediary countries, which will directly impact the licensing process.

# 10 HALLMARKS OF AN EFFECTIVE EXPORT COMPLIANCE PROGRAM

1. Executive Buy-In ("Tone at the Top")
2. Practicality
3. Culture of Compliance
4. Designated Compliance Officer
5. Consistent Due Diligence
6. Early Detection Measures
7. Hands-On Training
8. Pricing in Compliance
9. Consistent Program Reassessment
10. Effective Outside Counsel

## CASE STUDY

**Shipping goods to a foreign country with military influence**

➔

## SANCTIONS COMPLIANCE

# OVERVIEW

## WHAT ARE THE SANCTIONS LISTS?

- For a variety of reasons relating to national security, law enforcement, and the protection of basic human rights, the U.S. government maintains "sanctions" on certain individuals, entities, and countries.
- The objective of such sanctions is to economically isolate these individuals, entities, and countries, by generally prohibiting U.S. persons from conducting business, and trading, with them.
- Each set of sanctions is memorialized in a "list," which U.S. individuals and companies can use to determine whether the party with which they want to conduct business/trade has been sanctioned.

## OFAC'S SPECIALLY DESIGNATED NATIONALS LIST

- The majority of sanctions are enforced by the Office of Foreign Assets Control ("OFAC") at the U.S. Department of the Treasury.
- OFAC has aggregated all of its sanctions lists into one master list, which is referred to as the "Specially Designated Nationals List" (the "SDN List").
- The following slides will provide a brief overview of some of OFAC's sanctions lists, each of which is represented in the SDN List.

## THE SPECIALLY DESIGNATED NATIONALS LIST- THREE OFAC SANCTIONS PROGRAMS

- The List of Foreign Financial Institutions Subject to Part 561
  - List of foreign financial institutions that knowingly violate the Iranian Financial Sanctions Regulations
- The Foreign Sanctions Evaders List
  - List of (a) foreign individuals and entities determined to have violated, attempted to violate, conspired to violate, or caused a violation of U.S. sanctions on Iran and Syria, or U.S. sanctions pertaining to non-proliferation or anti-terrorism; and (b) foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions.
- The Sectoral Sanctions Identifications List
  - List of entities in the Russian financial and energy sectors that have been sanctioned.

## NON-SDN OFAC SANCTIONS LISTS

- The Palestinian Legislative Council List
  - List of individuals sanctioned on the basis that they are members of the Palestinian Legislative Council who were elected on the party slate of Hamas, or any other Foreign Terrorist Organization, Specially Designated Terrorist, or Specially Designated Global Terrorist.
- The Non-SDN Iranian Sanctions Act List
  - List of persons determined to have made certain investments in Iran's energy sector or to have engaged in certain activities relating to Iran's refined petroleum sector.

# DEPARTMENT OF COMMERCE AND DEPARTMENT OF STATE LISTS

- The Department of Commerce and Department of State maintain their own lists of proscribed parties:
  - Department of Commerce
    - ➢ The Denied Parties List
      - ❑ List of individuals and entities that have been denied export privileges.
    - ➢ The Unverified List
      - ❑ List of parties that are ineligible to receive items subject to the Export Administration Regulations by means of a license exception.
  - Department of State
    - ➢ The Nonproliferation Sanctions List
      - ❑ List of foreign individuals, private entities, and governments that have been sanctioned for engaging in proliferation activities.
    - ➢ The AECA Debarred List
      - ❑ List of entities and individuals that have been prohibited by the Department of State from participating directly or indirectly in the export of defense articles, including technical data and defense services.

# PENALTIES

- The penalties for violating U.S. sanctions programs vary from program to program, but the following examples demonstrate the seriousness with which the U.S. government treats sanctions violations:
  - The SDN List
    - **≤ $20M** and **30 years** imprisonment (criminal)
    - **≤ $83K** per violation of Trading With the Enemy Act (civil)
    - **≤ $250K** or twice the amount of the underlying transaction for violating the International Emergency Economic Powers Act (civil)
    - **≤ $1,414,020** per violation of the Foreign Narcotics Kingpin Designation Act (civil)
  - The Denied Parties List
    - **≤ $1M** per violation and **20 years** imprisonment (criminal)
    - **≤ $11K** per violation (administrative) and **≤ $120K** per violation in cases involving items controlled for national security reasons
    - Denial of export privileges

# COMPLIANCE STRATEGIES

Employment is key. When considering hiring an employee, must consider:

- Liability to local government, U.S., and/or employee's home country
- Employer location: Local, U.S., or third country
- Employee is U.S. national resident or third party national
- Independent contractor
- Assignment length

Money is King. Can you afford it?

- Ability to pay vendors/procurement
- Ability to pay personnel salaries
- Ability to provide subgrantees funding

# NOTABLE ENFORCEMENT ACTIONS

The American Steamship Owners Mutual Protection and Indemnity Association, Inc. (2013)

- The American Steamship Owners Mutual Protection and Indemnity Association, Inc., a non-profit international marine mutual insurance association, violated the Cuban Assets Control Regulations, the Sudanese Sanctions Regulations, and the Iranian Transactions Regulations by processing insurance claims involving Cuba, Sudan, and Iran.
- Total penalties: **$1,729,000 (settled for $348,000).**

# CASE STUDY

- The "charitable sector" has been exploited by terrorists to raise and move funds, and to provide logistical support, cover, and operational assistance.
  - Nonprofits have been "put on notice" and are thus expected to have knowledge and compliance protocols in place to combat the threat, including SCREENING.

| RISK FACTORS FOR CHARITIES DISBURSING FUNDS OR RESOURCES TO GRANTEES | | |
|---|---|---|
| **Low Risk** | **Medium Risk** | **High Risk** |
| The grantee has explicit charitable purposes and discloses how funds are used with specificity. | The grantee has general charitable purposes and discloses how funds are used with specificity. | The grantee has generable charitable purposes and does not disclose how funds are used. |
| The charity and the grantee have a written grant agreement that contains effective safeguards. For example, provisions addressing proper use of funds by the grantee. | The charity and the grantee have a written grant agreement with limited safeguards. | The charity and the grantee do not have a written grant agreement. |

# PRIVACY COMPLIANCE

# OVERVIEW

## DATA PRIVACY COMPLIANCE ISSUES

- General Data Protection Regulation (GDPR)
  - Broad application
  - Revenue-based fines
- Intellectual Property Rights
  - Trademark issues
  - Copyright concerns

## GENERAL DATA PROTECTION REGULATION (GDPR)

- The General Data Protection Regulation sets guidelines for the collection and processing of personal information of individuals within the European Union (EU), while also imposing fines that can be revenue-based.
- GDPR covers all companies that deal with data of EU citizens, which came into effect on May 25, 2018.
- It applies to all organizations that process personal data of European residents, whether or not they are physically located in Europe.

## PRIVACY COMPLIANCE: CONTROL INTELLECTUAL PROPERTY

- Trademark battles
  - Non-distinctive logos or marks
  - Costly buyouts
- Copyright
  - Standards (policies)
  - Programs (systems that work)

## PENALTIES

- Failure to comply with GDPR's requirements could result in fines of up to 4% of an organization's total revenue or 20,000,000 euros
- Losing your rights to logos and licenses
- Plagiarism

# COMPLIANCE STRATEGIES

- Consider registration of IP (or "international" version of IP) under local laws in target country
- Differentiating between IP and "confidential information," i.e., business proprietary info (also requires contractual protections)
- Registered IP: Logos, trademarks, certification marks, and patents
- Copyright material, such as standards
- Nonprofit managers might wish to consider whether they are eligible to participate in the Privacy Shield
- Individuals must also be advised of their rights
- Document compliance with the GDPR (i.e., record-keeping obligations, the use of privacy impact assessments, and the appointment of a data protection officer or EU legal representative)

# CASE STUDY

FocalPoint

Fostering Global Partnerships
Through Educational Technology

VS

.

University of Pennsylvania
INTERNATIONAL RELATIONS PROGRAM

QUESTIONS?