Guidepost

Export Controls and International Research

Society for Corporate Compliance and Ethics
2020 Virtual Higher Education Compliance Conference

June 3, 2020, 10:45 AM–12:15 PM CENTRAL TIME ZONE

Panelists: Julie Myers Wood, Chief Executive Officer, Guidepost Solutions, LLC
Robert F. Roach, founding Chief Global Compliance Officer & Vice President, New York University (2006-2020)

1

Guidepost

Introduction - Session Outline

Part 1. **U.S. Export Control and Trade Sanction Laws:** This session will provide a broad overview of key U.S. export control and trade sanction laws which may arise in the context of University activities, including international research.

Part 2: **Risk Mitigation and Collaborative Relationships:** The session will cover multiple ways in which university compliance officers, working with other university departments, can help mitigating compliance risks and develop effective compliance programs

Part 3: **Compliance Program Assessments:** Finally, we will touch on the importance of conducting periodic compliance program assessments, including self-assessments and third-party assessments.

Part 4: **Questions and Discussion**

2

Guidepost

Part 1: Overview

Key U.S. Export Control and Trade Sanction Laws

3

Guidepost

U.S. export control and economic sanctions laws are intended to support U.S. national security or foreign policy interests. University Compliance Officers should be familiar with three key U.S. regulatory regimes:

- The **International Traffic in Arms Regulations ("ITAR")** controls are aimed at regulating the export and import of military Items. The ITAR is administered by the Department of State, Directorate of Defense Trade Controls ("DDTC")

- **Export Administration Regulations ("EAR")** are aimed at limiting the export of so-called "dual use" Items that were intended for civilian purposes but that could also be used in military applications. The EAR is administered by the Department of Commerce, Bureau of Industry and Security.

Both the ITAR and the EAR also focus on the nationality of persons who may receive access to controlled technology within the United States under their respective "*deemed export*" rules.

Finally, both the ITAR and EAR also have a critical provision called the "*fundamental research exemption*" and other exemptions that help temper the regulatory burden of these export control laws.

4

Guidepost

Separate from these ITAR "*military*" and EAR "*dual use*" export controls are U.S. economic and trade sanctions rules.

- The **U.S. Treasury Department's Office of Foreign Assets Control ("OFAC")** regulations impose partial or comprehensive economic and trade related sanctions against certain designated countries, groups or individuals. OFAC regulations are designed to enforce U.S. policies against terrorism, proliferation of weapons of mass destruction, narcotics trafficking, human rights violations and other national security and other foreign policy considerations

These sanctions-related requirements cover all U.S. persons and all U.S.-origin items. The sanctions generally apply regardless of the technological content of any proposed international import or export transaction, because of major foreign policy differences between the United States and those countries, irrespective of whether they pose any actual or likely national security threat. As such, under these sanctions regulations, the precise nature or degree of technical content in the U.S. items is often irrelevant.

Moreover, unlike the ITAR and EAR export control regimes, these sanctions rules do not allow for any "*fundamental research exemption*" for U.S. institutions of higher education, but they do contain other provisions that are still useful and relevant for academic institutions, particularly in regard to the preparation, editing and publication of academic articles.

5

Guidepost

U.S. Persons vs. Foreign Persons

One common feature to all three U.S. export control and trade sanctions regimes is a clear distinction between those who are considered "U.S. persons" and "foreign persons."

In general, under these U.S. export control and trade sanctions laws:

- A "U.S. person" is any U.S. citizen, U.S. permanent resident alien or person admitted on an asylum status to the United States or a legal entity organized under U.S. law; and

- A "foreign person" (or "foreign national") is then any other type of individual or legal entity. Thus, foreign persons include foreign national students who are in the U.S. on an F-1 student visa, foreign national faculty or staff persons who are in the U.S. on an H-1B work visa, and visiting foreign scholars who are in the U.S. on J-1 visiting scholars' visas.

6

Guidepost

Export Control and Trade Sanction Laws Summarized in One Photo

Syrian rebels aim a mortar using an iPad.

7

Guidepost

Part 1 *(continued)*:
The EAR

Controls Related to "Dual Use" Technologies

8

Guidepost

Most U.S. Items, Technology and Software are “dual use” in nature and are covered under the EAR, 15 CFR Part 700 et seq., administered by the U.S. Commerce Department’s Bureau of Industry and Security (“BIS”).

The CCL: BIS has published a detailed list of Items that are considered controlled under the EAR. This list is known as the Commerce Control List (“CCL”). and is found in Supplement No. 1 to EAR Part 774. Using the CCL and the EAR’s Country Chart (found in Supplement No. 1 to EAR Part 738) one can determine whether a BIS export license is required to export a controlled Item to a particular end-user in a particular country.

This BIS website http://www.bis.doc.gov contains three specific lists of foreign individuals and entities that would be problematic for a U.S. exporter to deal with: the **Denied Persons List**, the **Entity List** and the **Unverified List.**

9

Guidepost

1. The **Denied Persons List** identifies those persons who have been officially denied export privileges by the BIS under punitive orders and is located at http://www.bis.doc.gov/index.php/the-denied-persons-list;
2. The **Entity List** is a list that sets forth foreign end-users known to be involved in proliferation activities and the development of weapons of mass destruction or missiles to deliver those weapons. Since its initial publication, grounds for inclusion on the Entity List have expanded to activities sanctioned by the State Department and activities contrary to U.S. national security and/or foreign policy interests. The Entity List is located at http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list; and
3. There is also a separate BIS **Unverified List** in which the BIS has named certain companies about which it has suspicions. U.S. exporters are not forbidden, as such, to deal with any of the persons or entities listed on the Unverified List, but such exporters and their international resellers should proceed quite cautiously in any transaction with a person or entity on that list. In the language of the BIS, being included on the Unverified List should raise a “red flag,” as further explained here: http://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/unverified-list.

10

Guidepost

What is an Export?

- Physical shipments abroad
- Transmitting or accessing abroad to U.S. technology or software
- Disclosure of technology or to a foreign national anywhere ("Deemed Export")

What is a Deemed Export?

Disclosure of "technology" to foreign national

- By oral or visual disclosure
- Occurring anywhere (in the U.S. or overseas)
- May occur through: Email, FTP, Tours or inspections, Conversations, Remote server access

11

Guidepost

EAR Decision Making

In essence, a U.S. exporter needs to use the EAR to make five determinations:

01 — Is the item, technology or software "subject" to the EAR or does an "EAR Exemption" apply?

02 — If subject to the EAR, is the item, technology, or software on the EAR's CCL?

03 — If on the CCL, above what functional level of power, performance, size or other parameter of the relevant technology must the BIS issue an "export license" before the sale can be made, and, conversely, below what level might a U.S. exporter ship the Item overseas under a "license exception" even if a license is nominally required by the CCL?

04 — Are there specific end-uses, end-users or destinations that require any different treatment in terms of licensing or handling?

05 — Does the EAR Country Chart indicate that an export to the nation of the end-user requires an export license

12

Guidepost

Key EAR Exemptions

Several Key EAR "Exemptions" that are helpful to Universities:

- **Fundamental Research Exemption (FRE):** A university can allow a foreign persons access to controlled technology under the FRE, which is defined as "technology" or "software" that arises during, or results from, fundamental research and is intended to be published, which is not subject to the EAR. "Technology" or "software" that arises during, or results from, fundamental research is intended to be published to the extent that the researchers are free to publish the "technology" or "software" contained in the research without restriction.
- **Exemption for Publicly Available Technology or Software**: "technology" or "software" is "published," and is thus not "technology" or "software" subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination (with the exception of certain encryption software classified under ECCN 5D002).
- **Exemption for University "Catalog Course" Information**: Are released by instruction in a catalog course or associated teaching laboratory of an academic institution.
- **Note:** these Exemptions do NOT apply to the export of **items** controlled for export by the CCL (e.g. export of prototypes developed during the course of Fundamental Research).

13

Guidepost

Preserving the EAR

Publication restrictions may invalidate "fundamental research"

- Examples:
  - Contract requires sponsor approval of publication
  - PI agrees not to involve foreign nationals
  - Side letter or agreements that restrict certain data from publication
- Examples of permitted review
  - Review to protect patent rights or proprietary data
  - SO LONG AS only a "temporary delay" in publication

14

Guidepost

Part 1 *(continued)*:

The EAR

Emerging Areas of Importance to Universities

15

Guidepost

The National Defense Authorization Act FY 2019

The National Defense Authorization Act FY 2019 (NDAA FY2019) was signed into law on August 13, 2019.

It includes provisions designed to limit foreign access to sensitive technologies and links together the **Export Control Reform Act of 2018 (ECRA)** and the **Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)** which were both incorporated into the NDAA FY 2019.

16

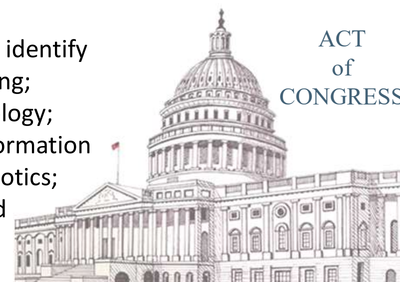
Guidepost

The Export Control Reform Act of 2018 (ECRA)

The ECRA gives the Department of Commerce, Bureau of Industry and Security (BIS) permanent statutory authority for the export administration regulations. It also establishes a new interagency process to identify and impose export controls on **"emerging and foundational technologies"** essential to the national security.

On November 19, 2018, BIS published an advanced notice of proposed rulemaking (ANPRM) seeking public comment to help identify and assess "emerging technologies" for purposes of updating the export control lists.

It includes a list of 14 representative technologies that will be assessed to identify "emerging technologies", including: biotechnology; AI and machine learning; position, navigation, and timing (PNT) technology; microprocessor technology; advanced computing technology; data analytics technology; quantum information and sensing technology; logistics technology; additive manufacturing; robotics; brain-computer interface; hypersonics; advanced materials; and advanced surveillance technologies.



17

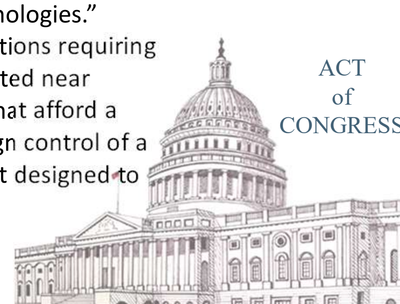
Guidepost

The Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA)

The Committee on Foreign Investments in the United States (CFIUS) is an interagency committee led by the Treasury Department that reviews transactions that could result in control of a U.S. business by a foreign person to determine the effect of the transaction on U.S. national security ("covered transactions").

FIRRMA expands CFIUS jurisdiction to address growing national security concerns over foreign exploitation of certain investment structures involving "critical technologies." FIRRMA expands the definition of a "covered transaction." Covered transactions requiring CFIUS review now include: transactions by foreign person in real estate located near sensitive government facilities; (2) investments in certain U.S. businesses that afford a foreign person access to material nonpublic technical information; (3) foreign control of a U.S. business (4) any other transaction, transfer, agreement, or arrangement designed to circumvent CFIUS jurisdiction.

Note: possible application to University startups and foreign investors



18

Guidepost

Emerging Technology: AI/Geospatial Imagery

On January 6, 2020, the US Department of Commerce's Bureau of Industry and Security (BIS) issued the first "emerging technology" rule to control artificial intelligence-based software specially designed to automate the analysis of geospatial imagery and point clouds. https://www.govinfo.gov/content/pkg/FR-2020-01-06/pdf/2019-27649.pdf
BIS added certain software specially designed to automate the analysis of geospatial imagery to ECCN 0D521. A license is required for the export and reexport of these items to all destinations, except Canada. Items under the "0Y521" series, including 05D21, remain in that ECCN for up to a year while the US Government determines whether classification under a revised or new ECCN, or an EAR99 designation, is appropriate.

This interim final rule controls geospatial imagery software specially designed for training a Deep Convolutional Neural Network to automate the analysis of geospatial imagery and point clouds, and satisfying all of the following criteria:

- Provides a graphical user interface that enables the user to identify objects, such as vehicles and houses, from within geospatial imagery and point clouds in order to extract positive and negative samples of an object of interest;
- Reduces pixel variation by performing scale, color, and rotational normalization on the positive samples;
- Trains a Deep Convolutional Neural Network to detect the object of interest from the positive and negative samples; and
- Identifies objects in geospatial imagery using the trained Deep Convolutional Neural Network by matching the rotational pattern from the positive samples with the rotational pattern of objects in the geospatial imagery.

19

Guidepost

Part 1 *(continued)*:

The ITAR

Emerging Areas of Importance to Universities

20

Guidepost

International Traffic in Arms Regulations (ITAR) controls technology that is intended mainly or exclusively for military purposes or that may have direct use in military applications. ITAR is administered by the U.S. State Department's Directorate of Defense Trade Controls ("DDTC") The ITAR are codified at 22 CFR Part 120 *et seq*.

The official DDTC website is located at www.pmddtc.state.gov and contains the current version of the ITAR.

The ITAR list of controlled military Items is known as **the United States Munitions List ("USML")**. The USML contains a list of ITAR-controlled "defense articles" and "defense services" and can be found at: www.pmddtc.state.gov/regulations_laws/itar_consolidated.html.

The State Department also maintains its own list of parties who are barred by ITAR Section 127.7 from participating directly or indirectly in the export of defense articles, including controlled technical data, or in furnishing of defense services for which a DDTC license or approval is required by the ITAR. That list of statutorily debarred parties under the ITAR is located at: www.pmddtc.state.gov/compliance/debar.html.

21

Guidepost

The ITAR sharply affects the procedure for exporting ITAR-controlled Items overseas, and that procedure is quite distinct from the process under the EAR:

- Affected exporters (and universities) who come within the DDTC's jurisdiction **must register annually with the DDTC** and must obtain a DDTC registration code.
- Identify and appoint an "empowered" ITAR official.
- Under ITAR, the **DDTC must also approve exports and contracts for technology transfers to foreign persons** before such exports or technology transfers can take place.
- As a general rule, if an Item is subject to the ITAR, then **any international transactions involving an ITAR Item will require prior DDTC export (or import) licensing** through its online D-Trade system.

22

Guidepost

The ITAR also has its own analogs to the EAR's ***"deemed export"*** and ***"FRE"*** rules in ITAR Sections 120.17(a)(2) and 120.11(a)(8), respectively. Under ITAR's deemed export rule "Any release in the United States of technical data to a foreign person is deemed to be an export to all countries in which the foreign person has held or holds citizenship or holds permanent residency."

Also, the protection of the ITAR's FRE ends as soon as a university or investigator proposes to send any ITAR-controlled technology or software outside the United States, either physically or electronically. At that point, the university and investigator must consider that export situation exactly as if it were an American company engaging in the same sort of proposed export and so must examine the ITAR's stringent export licensing requirements to confirm whether a DDTC export license must be obtained through its online D-Trade system.

It is also important to note that while the definition of FRE has been conformed under the EAR and ITAR, the FRE in ITAR is part of the "Public Domain" Exemption of ITAR for "information which is published and which is generally accessible or available to the public." That Exemption also provides in 120.17(a)(7) that public release of ITAR controlled technology in any form after approval by the cognizant U.S. government department or agency

23

Guidepost

Part 1 *(continued)*:

OFAC

Emerging Areas of Importance to Universities

24

Guidepost

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") administers a range of regulations that impose partial or total trade economic sanctions against certain designated countries, groups or individuals. These different sets of OFAC regulations are found at 31 CFR Part 500 *et seq.* These regulations are "foreign policy"-driven controls and can come into effect and be terminated or changed quite quickly, even abruptly and with little or no warning, by the U.S. Government in response to evolving geopolitical events.

- The country-based economic sanctions regimes such as those that target Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine, can be very rigorous and may bar almost any sort of import or export transaction with those countries or their governments. In addition to the text of each set of sanctions regulations, the OFAC website also often contains country-by-country explanations for each of the OFAC sanctions programs, written mostly in "plain English." The OFAC website is found at www.treas.gov/offices/enforcement/ofac/.
- OFAC also publishes lists of Specially Designated Nationals ("SDNs") and so-called "blocked persons" with whom it is illegal for U.S. persons to trade or do business. Those official lists can be found at www.treas.gov/offices/enforcement/ofac/sdn/index.shtml.

25

Guidepost

In contrast to the ITAR and the EAR, there is **no form of any FRE within any of the OFAC sanctions programs**.

However, the functional equivalent of the FRE might be obtained by a type of OFAC regulation that says, in effect,

- Certain preexisting informational materials.
- A foreign student or scholar lawfully admitted to study and do research at an American college or university is thereby allowed to do all that such foreign person's visa would allow him or her to do. *See, e.g.*, Iranian Transactions and Sanctions Regulation Section 560.505, which would apply to an Iranian national professor or student allowed to enter the United States to work or study at a specific institution.
- Individuals located in Iran, or located outside Iran but who are ordinarily resident in Iran, to sign up for and to participate in **undergraduate level online courses (including Massive Open Online Courses, coursework not part of a degree seeking program, and fee-based courses) provided by U.S. academic institutions in the humanities, social sciences, law, or business** or are introductory undergraduate level science, technology, engineering, or math courses ordinarily required for the completion of undergraduate degree programs in the humanities, social sciences, law, or business.

26

Guidepost

In addition, regarding all such OFAC-sanctioned countries, U.S. universities and scholars should be aware of unique OFAC concerns and legal requirements that affect common academic activities such as peer review, editing and publication of academic papers submitted by authors in OFAC-sanctioned countries such as Cuba and Iran, attendance and participation at academic conferences held in such OFAC-sanctioned countries and any active research collaborations, exchanges or other interactions with fellow scholars in such OFAC-sanctioned countries.

Unfortunately, the specific rules governing such issues will vary considerably from one OFAC sanctions regime to another, and those OFAC rules or policies are not always well publicized by OFAC. An American university facing such potential challenges should consult appropriate advisors to be sure they remain in compliance with these diverse OFAC rules.

27

Guidepost

Part 2:
Risk Mitigation and Collaborative Relationships

Working with Other Responsible University Departments to Mitigate Risk

28

Guidepost

U.S. Guidance on Effective Compliance Programs

The U.S. Departments of Commerce, State and Treasury have all issued guidance for establishing and sustaining effective compliance programs, including:

- EAR Compliance Programs - https://www.bis.doc.gov/index.php/documents/pdfs/1641-ecp/file
- ITAR Compliance Programs - https://www.pmddtc.state.gov/ddtc_public?id=ddtc_kb_article_page&sys_id=4f06583fdb78d300d0a370131f961913
- OFAC Compliance Programs - https://www.treasury.gov/resource-center/sanctions/Documents/framework_ofac_cc.pdf

In Part 2 of this program we will use the OFAC guidance as an example to review the importance of using a risk-based approach to export and trade compliance, in close collaboration with other responsible university departments to establish and sustain effective compliance processes and programs.

29

Guidepost

OFAC Guidance on Compliance Programs

OFAC strongly encourages organizations subject to U.S. jurisdiction, as well as foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, to employ a risk-based approach to developing, implementing, and routinely updating a sanctions compliance program

It is important to note that the nature and extent of an organizations compliance program will vary depending upon the nature of its activities and the specific risks it faces, including the organization's size and sophistication; the nature of its activities, services, and customers/clients, and its geographic locations—OFAC recommends that each program should be predicated on and incorporate at least five essential components of compliance:

1 Risk assessments

2 Management commitment

3 Internal Controls

4 Training

5 Testing and auditing

30

Guidepost

Why a Risk-Based Approach to Compliance

Risks in sanctions compliance are potential threats or vulnerabilities that, if ignored or not properly handled, can lead to violations of OFAC's regulations and negatively affect an organization's reputation and business.

OFAC recommends that organizations take a risk-based approach when designing or updating a Sanctions Compliance Program. One of the central tenets of this approach is for organizations to conduct routine, and if appropriate, ongoing "risk assessment" process for the purposes of identifying potential OFAC issues they are likely to encounter.

The results of a risk assessment are integral in informing the Sanctions Compliance Program's policies, procedures, internal controls, and training in order to mitigate such risks. According to OFAC , risk assessments "**should generally consist of a holistic review of the organization from top-to-bottom and assess its touchpoints to the outside world."** This process allows the organization to identify potential areas in which it may, directly or indirectly, engage with OFAC-prohibited persons, parties, countries, or regions. **Thus, close collaboration with University Departments whose activities may touch upon potential OFAC Sanction issues are critical.**

31

Guidepost

Risk Assessment Process

Analyze and understand your University's business/academic processes that may give rise to possible OFAC sanction issues. Possible areas or activities to consider include:

- **Procurement** – Vendor relationships, procurement of export controlled items
- **Finance** – International banking, payments and money transfers
- **Admissions/Registrar** – Students, including foreign national undergraduate and graduate students
- **Immigration Services** – Foreign students and visiting scholars on U.S. visas, international travel
- **Human Resources** – Employees, including foreign national employees
- **Research Administration** – Research grants, contracts and projects, particularly international research
- **Office of Industrial Relations** – IP, NDAs, MTAs, corporate sponsored research, and start-ups
- **Development** – Gifts from individuals, organizations, particularly foreign grants and gifts supporting research
- **Shipping and Logistics** – particularly International shipments of goods
- **IT** – Data Storage, Data Transfer, access to High Performance Computing remotely and by international researchers
- **Foreign Campuses and Programs** – must be integrated into overall compliance programs and processes

Working closely with department heads and process owners is not only critical to conducting effective risk assessments, but also to implement effective internal controls, training programs, lines of communication across functions, and to senior management.

32

Guidepost

Importance of Collaborative Relationships

OFAC notes in its guidance that while each organization should design, develop, and implement its risk-based Sanction Compliance Program based on its own characteristics, “several organizations subject to U.S. jurisdiction have committed apparent violations due to a de-centralized Sanction Compliance Programs, often with personnel and decision-makers scattered in various offices or business units.”

The lack of sufficient coordination in decentralized compliance structures resulted in violations due to an improper interpretation and application of OFAC’s regulations, the lack of a formal escalation process to review high-risk or potential OFAC customers or transactions, an inefficient or incapable oversight and audit function, or miscommunications regarding the organization’s sanctions-related policies and procedures.

Universities are decentralized by nature, but with proper levels of collaboration and coordination of compliance efforts, effective Sanction Compliance Programs that meet OFAC standards can be developed and sustained.

33

Guidepost

Management Commitment

According to OFAC, senior management’s commitment to, and support of, an organization’s risk-based Sanctions Compliance Program is one of the most important factors in determining its success. This support is essential in ensuring the Sanctions Compliance Program receives adequate resources and is fully integrated into the organization’s daily operations, and also helps legitimize the program, empower its personnel, and foster a culture of compliance throughout the organization.

OFAC states that management commitment also helps insure that there are sufficient internal control functions to support the organization’s Sanction Compliance Program—**including but not limited to information technology software and systems**—that adequately address the organization’s OFAC-risk assessment and levels.

To the extent information technology solutions factor into the organization’s internal controls, the organization has selected and calibrated the solutions in a manner that is appropriate to address the organization’s risk profile and compliance needs, and the organization routinely tests the solutions to ensure effectiveness.

34

Guidepost

Information Technology: Screening Software

Before a university enters into any serious activities with any foreign person, exports any product or technology to any foreign person or obtains or provides services with a new foreign party, agent, supplier or vendor, university personnel should ensure that such foreign partner, party, customer, agent, supplier or vendor (collectively, “Proposed Party”) does not appear on any of the US government sanctions lists, including BIS, DDTC and OFAC sanctioned parties lists.

To do so, university personnel should review the lists through the available commercial tool used by the university or, at a minimum, the federal Consolidated Database to determine if the Proposed Party matches an entry on any of the Lists. Because the Lists are frequently updated but not on any set schedule, it is important that a university always check such a Proposed Party against the most current version of its commercial search tool or the Consolidated Database that appears on the website listed above. Using archived or stored copies of the commercial tool’s database or the Consolidated Database or of the Lists may provide out-of-date and invalid search results. **Note: Compare ad hoc use of screening software with screening software integrated into University computer systems and processes**

Because entries on the Lists often include specific identifying information (*e.g.*, full name, address, nationality, passport or tax identification number, place of birth, date of birth, former names and aliases, etc.), before reviewing the Consolidated Database, reviewing university personnel should gather as much identifying information about the Proposed Party as possible. In addition, university personnel should determine reasonable variations on the Proposed Party’s name.

35

Guidepost

Software Screening Process

To review a commercially available search tool or the Consolidated Database as a compliance resource, university personnel should generally follow the process below:

Review and “search” the resource to determine if the Proposed Party appears on any of the Lists. Use portions of the name(s) and other identifying information that the university has obtained to determine if a potential match exists.

Evaluate the quality of any possible matches by comparing the name listed with the name and other identifying information for the Proposed Party. (For instance, if the name of the Proposed Party is an individual while the listed name is a vessel, organization or company (or vice-versa), then there is not a valid match.)

Determine how much of the listed name matches the name of the Proposed Party. If the full name or a reasonably significant portion thereof matches, then continue to the next step. If not, then there is not a valid match.

36

Guidepost

Software Screening Process (Continued)

Compare the complete entry on the resource with the identifying information, if any, obtained from the Proposed Party.

a. If insufficient identifying information is provided on the resource or if any of the identifying information on the resource matches that of the Proposed Party, then continue to the next step.

b. If the information on the resource does not match that of the Proposed Party but the name is an exact match, then university personnel should notify the university's Export Control Compliance Officer (who can consult with outside counsel, if necessary, to determine if there is a likely match or not).

c. If there is a potential or exact match between an entry on the resource and a Proposed Party, then university personnel should notify the appropriate Export Control Compliance Officer or legal counsel.

37

Guidepost

Part 3:
Compliance Program Assessments

38

Guidepost

Conducting Regular Compliance Program Assessments

According to OFAC guidelines, organizations should conduct independent audits or assessments of the effectiveness of their sanctions compliance processes and check for inconsistencies between these and day-to-day operations.

A comprehensive and objective testing or auditing ensures that an organization identifies program weaknesses and deficiencies, and it is the organization's responsibility to enhance its program, including all program-related software, systems, and other technology, to remediate any identified compliance gaps. Such enhancements might include updating, improving, or recalibrating SCP elements to account for a changing risk assessment or sanctions environment. Testing and auditing can be conducted on a specific element of an SCP or at the enterprise-wide level.

OFAC advises that the testing or audit function should accountable to senior management, independent of the sanctions compliance program and audited functions. The assessments can be conducted internally or by an external party, but the persons conducting the review should have sufficient, skills, expertise, resources and the assessment process should reflects a comprehensive and objective review of the organization's Sanctions Compliance Program.

39

Guidepost

Outside Experts

At NYU, we have utilized outside experts to assist with our export control and trade sanctions compliance programs in a variety of ways:

- Working with responsible university departments, helped us choose our sanctions screening software and implement an automated the screening process
- Maintain and develop screening processes
- Conduct comprehensive independent reviews of export and trade control processes
- Provide ongoing assistance with resolution of complex or sensitive issues as they arise

40

Guidepost

Questions?

41