Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

InfoPAK[SM]

Complying With United States Export and Sanction Laws and Regulations

Sponsored by:

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

Complying With United States Export and Sanction Laws and Regulations

Updated November 2013

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This InfoPAK[SM] addresses United States laws imposing export controls and economic and trade sanctions. These laws and their implementing regulations can present unique challenges to businesses because they are complex and often can be counter-intuitive to the business person. Nevertheless, U.S. government enforcement agencies expect companies to know the rules governing cross-border commerce. An increasing number of companies are being held accountable for violations of export and sanctions laws, and are receiving ever-increasing penalties.

As markets, supply chains and workforces become more global, more and more businesses are confronted with the need to comply with these laws. However, the diversity and complexity of the laws and, even more so, their implementing regulations can make benchmarking obligations and adopting sensible internal compliance mechanisms a difficult endeavor. Although recent and anticipated reforms promise to simplify compliance burdens under these laws, the burdens will remain complicated and challenging.

The information in this InfoPAK should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of Womble Carlyle Sandridge & Rice, LLP, or of the Association of Corporate Counsel ("ACC") or any of their lawyers, unless so stated. Further, this InfoPAK is not intended as a definitive statement on the subject. Rather, this InfoPAK is intended to serve as a tool for readers, providing practical information to in-house practitioners.

The information contained in this InfoPAK was developed by **Womble Carlyle Sandridge & Rice, LLP**, the 2013 Sponsor of the ACC Compliance & Ethics Committee. For more information about Womble Carlyle, please see the "About the Author" section of this InfoPAK.

Contents

I. The Export Control Reform Initiative 10

II. Understanding Export and Sanctions Controls 10

A. Basic Guidance for Assessing Export Transactions 11

B. You May Be an Exporter and Not Even Know It 12

1. The Crossroads of Technology and Export/Sanctions Controls 12

2. How an Employer Becomes an Exporter 13

3. Even Non-U.S. Technology Can Become Subject to U.S. Controls 13

III. The Policies Behind Export and Sanctions Controls 14

IV. Dealing with Multiple Enforcement Agencies 15

A. The Primary Export/Sanctions Regimes 15

1. The Export Administration Regulations 15

2. The International Traffic in Arms Regulations 15

3. The Foreign Assets Control Regulations 16

B. Determining Which Agency Has Jurisdiction 16

C. The Changing Jurisdictional Landscape under the Export Control Reform Initiative 17

D. Coordinating Multiple Enforcement Agencies 17

V. Export Administration Regulations 17

A. The CCL's New 600 Series 17

B. Scope of the EAR: "Subject to the EAR" 18

C. Commerce Control List and Country Chart 18

D. General Prohibitions 19

1. Overview of the General Prohibitions 19

2. Guide to Using the General Prohibitions 20

E. Applying for a License 27

F. Dual Licensing Considerations 27

G. NLR ("No License Required") 27

H. Note about *De Minimis* 28

I. License Exceptions 28

J. Controls on Encryption Products and Technology 29

K. Antiboycott Controls 30

1. Prohibited Actions in Furtherance of a Boycott 30

2. Identifying Boycott Requests 31

3. Withholding Responsive Actions 32

4. Limiting Exposure from Third Parties 33

5. Other International Boycotts 33

M. Definitions of Key EAR Terms 33

1. Applicant 33

2. Category 33

3. Commerce Control List 34

4. Commodity 34

5. Countries Supporting International Terrorism 34

6. Country Chart 34

7. Country Groups 34

8. Designed or Modified 34

9. Development 35

10. Dual Use 35

11. Encryption Component 35

12. Encryption Items 35

13. Encryption Licensing Arrangement 35

14. Encryption Object Code 35

15. Encryption Software 35

16. Encryption Source Code 36

17. End-User 36

18. Export 36

19. Export Control Classification Number ("ECCN") 36

20. Exporter 36

21. Firm 36

22. Foreign Government Agency 36
23. General Prohibitions 37
24. Intermediate Consignee 37
25. Item 37
26. Knowledge 37
27. License 37
28. Licensee 37
29. License Exception 37
30. Object Code or Object Language 38
31. Open Cryptographic Interface 38
32. Person 38
33. Production 38
34. Production Equipment 38
35. Publicly Available Information 38
36. Publicly Available Technology and Software 39
37. Purchaser 39
38. Reasons for Control 39
39. Re-export 39
40. Required 39
41. Return without Action ("RWA") 39
42. Robot 40
43. Schedule B Numbers 40
44. Software 40
45. Source Code or Source Language 40
46. Space Qualified 40
47. Specially Designed 40
48. Subject to the EAR 41
49. Technical Assistance 41
50. Technical Data 41
51. Technology 41

52. Transfer 41
53. Ultimate Consignee 41
54. United States 41
55. U.S. Person 42
56. Use 42

VI. International Traffic in Arms Regulations 42

A. The ECR Initiative and the ITAR 42
1. Revised Categories 42
2. Transition Plan 43
3. Reexport/Retransfer of USML Items that have Transitioned to the CCL 44
B. Registering under the ITAR 44
C. Defense Articles and Defense Services 45
1. Defense Articles 45
2. Defense Services 47
D. Licenses and Agreements 47
1. Equipment Exports 47
2. Technical Data Transfers 48
3. Agreements 49
4. Comprehensive Authorizations 50
5. Temporary Imports of Defense Articles 50
E. Empowered Officials and Certifications 50
F. Congressional Notification 50
G. Political Contributions, Fees and Commissions 51
H. Definitions of Key ITAR Terms 51
1. Accessories and Attachments (§121.8(c)) 51
2. Broker (§129.2) 51
3. Brokering Activities (§129.2) 51
4. Build to Print (§124.13) 51
5. Component (§121.8(b)) 52
6. Defense Article (§120.6) 52

7. Defense Service (§120.9) 52
8. Empowered Official (§ 120.25) 52
9. End-Item (§121.8(a)) 53
10. Export (§120.17) 53
11. Firmware (§121.8(e)) 53
12. Foreign Person (§120.16) 54
13. Major Defense Equipment (§120.8) 54
14. Manufacturing License Agreement (§120.21) 54
15. Part (§121.8(d)) 54
16. Person (§120.14) 54
17. Public Domain (Including Fundamental Research) (§120.11) 55
18. Re-export and Retransfer (§120.19) 55
19. Significant Military Equipment (§120.7) 55
20. Software (§121.8(f)) 56
21. System (§121.8(g)) 56
22. Subject to the Export Administration Regulations (§120.42) 56
23. Technical Assistance Agreement (§120.22) 56
24. Technical Data (§120.10) 56
25. U.S. Person (§120.15) 57

VII. The OFAC Regulations 57

A. Proscribed Countries 57
B. "Nationals" and "Specially Designated Nationals" 58
C. What Activity/Conduct Is Prohibited 58
D. Permissible Letters of Intent and Discussions 59
E. Licensing Procedure under OFAC Regulations 59
F. Definitions of Key Terms under OFAC Regulations 59
1. Foreign Country 59
2. National 60
3. Nationals of More Than One Foreign Country 60
4. Specially Designated National 60

5. Person 60
6. Transactions 60
7. Transfer 60
8. Property 60
9. Interest 61
10. Person Subject to the Jurisdiction of the U.S. 61
11. Person within the U.S. 61

VIII. Enforcement of U.S. Export Control Laws 61

A. Statutory Penalties 61
B. What Constitutes a Violation 62
C. Contractual Duties of Government Contractors 62
D. Role of Voluntary Disclosures 63
E. Enforcement of Export and Sanctions Laws in Other Countries 64

IX. Developing an Internal Compliance Program 64

A. An Internal Compliance Program Must Be Credible 65
B. Assessing the Company's Unique Compliance Obligations 66
C. Molding the Compliance Program to the Company's Needs 67
D. Components of an Effective Compliance Program 68
1. Buy-in from Company Leadership 68
2. A Workable Structure and Designation of Focal Points 68
3. Education and Training 72
4. Screening 73
5. Diversion Avoidance and "Red Flags" 74
6. Instilling a Culture of Communication 76
7. Internal Audits 77
8. Recordkeeping 78
9. Notification, Reporting, and Internal Investigations 81
E. Compliance Challenges: Anticipating Unexpected Exports 82
1. Sales and Marketing Proposals 82
2. Attending Trade Shows 84

3. Foreign Travel 86
4. Posting Data on the Internet 87
5. Computer Security 87
6. Cloud Computing 88
7. Foreign National Visitors 89
F. Overview of an Internal Compliance Program 89
1. Key Elements 89
2. Element-By-Element Summary 90
X. About the Author 96
XI. Additional Resources 97
XII. Endnotes 98

I. The Export Control Reform Initiative

At the time of publication of this InfoPAK, President Obama's Export Control Reform ("ECR") initiative has begun rolling out with the implementation of a limited number of final rules that revise the export regulatory schemes. These rules are the first in what promises to be extensive revisions attempting to minimize gaps in inter-agency coordination, disagreements over commodity jurisdiction, and inefficiencies in the export licensing process. The ECR initiative also aims to balance national security with the growth of export industries by focusing government resources on those items warranting stricter control, and lessening controls on other items. The ECR initiative proposes to address these issues by ultimately establishing:

- A single export control licensing agency;
- A unified control list;
- A single enforcement coordination agency; and
- A single integrated information technology system.

Ultimately, the ECR initiative seeks to unify the major export regulatory schemes into one positive, tiered, and aligned list. So far, only the first steps have been taken towards this goal.

II. Understanding Export and Sanctions Controls

The United States controls the export of U.S. products, technology, and software to foreign countries and foreign persons. The U.S. also imposes economic and trade sanctions targeting specific countries, persons, and entities.

Two primary export control regimes exist under U.S. law – the Export Administration Regulations ("EAR") administered by the U.S. Department of Commerce, and the International Traffic in Arms Regulations ("ITAR") administered by the U.S. Department of State. These export regimes govern:

- Direct exports from the U.S.;
- Re-exports of U.S. products, technology, and software already abroad;
- Re-exports from locations outside the U.S. of non-U.S. made products incorporating more than a *de minimis* amount of U.S. content; and
- Re-exports from locations outside the U.S. of non-U.S. made products, which are derived from U.S. technology.

In addition, U.S. law imposes economic and trade sanctions on designated countries, entities, and persons. The Foreign Assets Control Regulations, administered by the U.S. Department of Treasury, is the primary sanctions regime, which includes restrictions on exports and many other transactions with persons and entities subject to the sanctions.

A. Basic Guidance for Assessing Export Transactions

To understand obligations under U.S. export controls, one must understand what an "export" is. Although the definitions are somewhat different under the EAR and the ITAR, both regimes broadly construe the term "export" to include:

- Sending or taking an article out of the United States in any manner;
- Transferring possession, control or ownership of certain defense articles to a foreign person, whether in the United States or abroad;[1] and
- Disclosing (including oral or visual disclosure) or transferring (including facsimile, mail, or e-mail transfer) controlled technical data to a foreign person, whether in the United States or abroad.

But, recognizing an export is only the starting point. To ascertain whether a particular export transaction is subject to prior licensing or other requirements under U.S. law, an exporter must know which export regime applies to the article and technology at issue in the transaction. Each export regime has its own unique requirements and compliance challenges. In order to make this assessment, exporters must know what item is being exported and the use or purpose to which it will be put.

After making this jurisdictional determination, however, the exporter must then assess four key issues underlying successful compliance with U.S. export controls:

- How the item being exported is classified under the applicable export regime;
- The destination where the item is being exported;
- The person or entity to whom the item is being sent; and
- The intended use of the item.

Depending upon the answers to these questions, the exporter may need to obtain license authorization to proceed with the export – ***prior to the export***.

The importance of complying with export and sanctions laws cannot be overemphasized. The U.S. government aggressively enforces these laws. Potential penalties for violations are severe, and include both civil and criminal penalties. Also, exporting is a privilege, not a right; violations can cause a business to forfeit this privilege.

B. You May Be an Exporter and Not Even Know It

1. The Crossroads of Technology and Export/Sanctions Controls

Technology has turned many companies into "exporters" under U.S. law, even where the company never ships commodities across borders. Technology, including software source code and any form of technical data, is like any other commodity under U.S. export laws – ***transferring technology to a foreign person wherever they are located is an export and may require prior approval***.

The challenges of complying with export controls are compounded by the many forms technology can take. Technology controlled under U.S. law includes technical data for the design, development, production, manufacture, assembly, operation, repair, maintenance, modification, or testing of controlled items; blueprints, drawings, photographs, plans, instructions and other documentation relating to controlled items; software source code; and technical assistance and services, such as instruction, skills building, training, and working knowledge relating to controlled items.

Not all information is controlled technology under U.S. law. Information in the public domain and general scientific, mathematical, or engineering principles typically found in treatises or taught in schools or universities, basic marketing information regarding function or purpose, or general system descriptions of articles are not controlled.

The many ways in which technology can be exported also complicates compliance efforts. An export of technology occurs by:

- Sending or taking technical data abroad in any form, including written, downloaded onto a laptop, or displayed in models or mock-ups;
- Communicating with foreign nationals in person, on the telephone, by e-mail, or by regular or express mail;
- Providing "know how," such as performing services or rendering assistance;
- Making presentations at conferences or elsewhere;
- Submitting articles for publication;
- Distributing brochures or presenting trade show displays; or

- Placing information on the internet

Because it can take weeks or months to obtain licenses from the government, it is important to consider export requirements early in transactions involving foreign persons. If a license is required, it must be obtained ***prior to*** any transfer or disclosure of technology.

2. How an Employer Becomes an Exporter

Under the so-called "deemed export" rule, the disclosure of technology to a foreign national[2] is deemed to be an export of that technology to the foreign national's country. The rule assumes that information disclosed to a foreign national can never be retrieved.

The "deemed export" rule is very broad. The unsuspecting employer may unwittingly find that it is an "exporter" under U.S. law because of the definition of foreign national existing under the export regulations. A foreign national is any person who is not a U.S. citizen or a permanent resident. Therefore, a person in the United States on a non-resident visa, such as B, L, H-1B is a foreign national, even if the visa comes with authorization to hold employment. Unless an exception applies, or the export is permitted on a "no-license-required" basis, prior government approval is required before controlled technology can be disclosed to that employee.

This can present problems for the employer. Until a license has been obtained, a foreign national employee may not access controlled technology. Only when a license is in place is s/he approved to receive technology, and even then, only unclassified technology and only to the extent requested in the application and approved in the license.

Currently, a petitioning employer sponsoring a nonimmigrant worker is required to certify on Form I-129, "Petition for a Nonimmigrant Worker," that it has reviewed the EAR and the ITAR and has made a determination whether an export license will be required for the release of technology to the nonimmigrant beneficiary.

The "deemed export" rule also applies to foreign national visitors or business colleagues to whom controlled technology will be disclosed. Also, U.S. persons who are employees of a foreign company or acting on behalf of a foreign entity should be treated as foreign nationals for purposes of U.S. export and sanctions controls. No transfers of technology should be made to these persons before assessing export/sanctions requirements.

3. Even Non-U.S. Technology Can Become Subject to U.S. Controls

Technology brought to the U.S. from another country is subject to U.S. laws while here. Restrictions on U.S. person transactions under sanctions programs include transactions involving such technology. Moreover, if the technology is exported from the United States, it will be subject to export licensing restrictions unless it is returned to its original source unchanged. Any changes to the content of the technology – other than non-substantive changes such as editorial comments – trigger U.S. export controls.

III. The Policies Behind Export and Sanctions Controls

U.S. export and sanctions laws implement various national policies, such as:

- **National Security.** It is U.S. policy to restrict the export of goods and technology which would make a significant contribution to the military potential of any other country or countries, and which would prove detrimental to U.S. national security.

- **Foreign Policy and Nonproliferation.** U.S. policy restricts the export of goods and technology as necessary to further U.S. foreign policy or to fulfill U.S. international obligations, such as nonproliferation of nuclear, chemical and biological weapons, and missile technology.

- **Short Supply.** It is U.S. policy to restrict the export of goods where necessary to protect the domestic economy from excessive drain of scarce materials and to reduce the serious inflationary impact of foreign demand.

- **Multilateral International Controls.** The U.S. Government is a party to international treaties and other arrangements imposing specific controls which are incorporated into U.S. laws and regulations. These multilateral regimes include: (i) The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, which requires members to enforce controls on specified items and technology; (ii) The Missile Technology Control Regime, which controls proliferation of missile delivery systems for use with nuclear, chemical, and biological weapons; (iii) The Chemical Weapons Convention, which bans development, production, possession, transfer and use of chemical weapons, and The Australia Group which has established multilateral controls over chemical precursors and production equipment, biological processing equipment and related technical data; and (iv) The Nuclear Suppliers Group, which coordinates multilateral export controls on dual-use items with applications in nuclear weapons design and development.

Not surprisingly, these policies often confront competing policies, and tensions can arise. The policies underlying export/sanctions controls compete with national interests in freedom of trade, maximizing exports, creation of U.S. jobs, encouraging U.S. investments abroad, freedom of speech, and academic freedom. Resolution of these tensions sometimes leads to inconsistent enforcement priorities.

IV. Dealing with Multiple Enforcement Agencies

There are three primary export/sanctions regimes that will be covered in these materials, and each regime is enforced by a different agency – the Departments of State, Commerce, and Treasury. However, many other federal agencies administer regulations controlling specific types of exports in their areas of regulatory competence, including the Drug Enforcement Agency, Agriculture Department, Fish and Wildlife Service, Environmental Protection Agency, Maritime Administration, Department of Energy, Nuclear Regulatory Commission, Patent and Trademark Office, Food and Drug Administration, and Consumer Product Safety Commission.[3] Although not covered here, exporters whose products are regulated by these agencies must be aware of these controls.

A. The Primary Export/Sanctions Regimes

The primary export and sanctions regimes are the Export Administration Regulations, the International Traffic in Arms Regulations, and the Foreign Assets Control Regulations. Each will be briefly summarized here.

1. The Export Administration Regulations

The EAR[4], promulgated under the authority of the Export Administration Act[5], control the export from the United States of certain commercial commodities, software, and technology. The EAR are administered by the U.S. Department of Commerce's Bureau of Industry & Security ("BIS"). The EAR govern export of controlled commodities and data through a series of prohibitions giving effect to U.S. policies. Before exporting any controlled commodities or technology, an exporter must assess the proposed transaction against the prohibitions to determine if the transaction requires U.S. government approval and, if so, obtain the approval. The EAR also include regulations, administered by the U.S. Department of Commerce's Office of Antiboycott Controls ("OAC"), prohibiting participation in boycotts or restrictive trade practices against countries friendly to the United States.

2. The International Traffic in Arms Regulations

The ITAR[6], promulgated under the authority of the Arms Export Control Act ("AECA")[7], control the export of defense articles, technical data and services from the United States to foreign destinations and persons. The ITAR are administered by the U.S. Department of State's Directorate of Defense Trade Controls ("DTC"). A "defense article" is any item specifically listed on the United States Munitions List ("USML")[8] or which has been adapted or configured for a military purpose or to conform to a military specification. A "defense article" is more than just weapons, and includes electronics systems, information technologies systems, and a variety of novel "adapted" items. The ITAR control the export of not only defense articles, but also defense services and technical data directly related to defense articles.

3. The Foreign Assets Control Regulations

The Foreign Assets Control Regulations ("FACR")[9], promulgated under the authority of the International Emergency Economic Powers Act ("IEEPA")[10] and the Trading with the Enemy Act ("TWEA")[11], implement economic and trade sanctions based on U.S. foreign policy and national security goals against targeted countries, individuals, and entities identified by the U.S. government as engaging in terrorist, weapons-proliferating or narcotics-trafficking activities. Administered by the U.S. Treasury Department's Office of Foreign Assets Controls ("OFAC"), the regulations prohibit specified transactions and activities by U.S. persons and entities wherever located and, in some cases, by foreign subsidiaries and branches of U.S. companies.

B. Determining Which Agency Has Jurisdiction

Determining which agency has jurisdiction over a transaction is a necessary threshold step in complying with the U.S. export and sanctions laws. The OFAC regulations, where they apply, override the EAR and the ITAR. Exports that may be permitted under those regimes, even with license restrictions, may be subject to sanctions which "trump" exports authorized under their regulations.

But, where the OFAC regulations do not apply, determining whether the EAR or the ITAR have jurisdiction over an item intended for export can be fraught with uncertainty. The coverage of the EAR and ITAR sometimes overlaps. Also, jurisdiction over whole categories of items may be suddenly transferred between the two agencies, depending upon then-current assessments of the level of controls needed for a particular item.

Exporters who can confidently rely on their own self-assessment of jurisdiction should carefully review the applicable regulations and document their assessment accordingly. However, if there is any doubt as to which export regime controls, exporters should consider filing a "Commodity Jurisdiction Request" with DTC to obtain a formal determination whether the item is subject to the ITAR.[12] A copy of the request should also be filed with BIS. A formal jurisdiction determination by DTC is protection against a later allegation of having violated licensing requirements.

Under current guidelines, commodity jurisdiction determinations should be completed by DTC in no more than sixty (60) days following submission by an exporter of a formal request. Previously, commodity jurisdiction determinations were completed in ninety (90) days.

An exporter with multiple products or technologies should consider developing and maintaining an internal matrix showing how these items are classified under the applicable regime. The matrix should be updated as new products or technologies are introduced, and as regulatory changes occur. Periodic regulatory updates or revisions can alter how products and technologies are controlled for export purposes.

C. The Changing Jurisdictional Landscape under the Export Control Reform Initiative

In rules finalized simultaneously by BIS and DTC on April 16, 2013, the first substantive steps in the President's ECR initiative were taken with the announcement that munitions items no longer deemed necessary to be included on the USML would move to the Commerce Control List ("CCL") on October 15, 2013. Under these new rules, new "600-series" Export Control Classification Numbers ("ECCNs") have been added to each applicable CCL category to capture all defense articles moving from the USML to the CCL. Additionally, the final rules adopt a new definition of the term "specially designed," which is important for classifying articles that move to the CCL.

D. Coordinating Multiple Enforcement Agencies

As part of the ECR initiative, President Obama ordered the creation of the Export Enforcement Coordination Center ("E2C2"). The objective of E2C2 is to create a single enforcement coordination center, in line with the goal of creating a single control list, a single licensing agency, and a common IT system. Several agencies are entitled to investigate potential export control violations and enforce appropriate penalties. Administered by the Department of Homeland Security ("DHS"), E2C2's role is to coordinate enforcement activities among these several agencies by sharing information and reducing the duplication of investigation and enforcement efforts. The agencies that are participating in E2C2 are the Director of National Intelligence, and the Departments of Justice, Commerce, State, Treasury, Defense, Homeland Security, and Energy.

V. Export Administration Regulations

A. The CCL's New 600 Series

The creation of the "600 Series" ECCNs within the CCL ("600 Series") is one of immediate importance for exporters generally. Intended to reduce the burdens of licensing requirements for certain items, the 600 Series will control those items on the CCL previously controlled by the USML, or that are covered by the Wassenaar Arrangement Munitions List ("WAML"). An ECCN for an item covered by the 600 Series would appear as "xY6zz" with "x" indicating the CCL category, "Y" indicating the CCL subcategory, "6" denoting the 600 series, and "zz" indicating the fourth and fifth characters of the WAML.

The 600 Series also introduces a sixth character (*e.g.*, "xY6zz.a") intended to indicate subcategories for classifying items moving from the USML to the CCL. They are as follows:

- The ".a – .w" subparagraphs include specifically enumerated end items, parts, components, accessories, and attachments (collectively, "Items"). Items in this subparagraph will have strict license requirements.

- The ".x" subparagraph includes items and software that are *not* enumerated on the new USML or in subparagraphs ".a – .w," *and* which are "specially designed" for an item enumerated on the USML or in the corresponding 600 series. (*See Definitions: "Specially Designed"*). Items in this subparagraph will have strict license requirements.

- The ".y" subparagraph includes specifically enumerated parts, components, accessories, and attachments that only warrant "AT-only" controls (i.e., controls for antiterrorism reasons).

If the item in question is covered by the ".y" subparagraph, *e.g.* with a classification of "xY6zz.y," the item is subject only to AT controls and would permit exports to most destinations without a license. If the item in question is *not* covered by the ".y" subparagraph, but is covered by either the ".a – .w" or ".x" subparagraphs, a license will be required for export to all destinations except Canada unless a license exception is available.

The 600 Series and the term "specially designed" are further explained in Supplement No. 4 to Part 774 of the EAR (CCL Order of Review).[13]

B. Scope of the EAR: "Subject to the EAR"

The threshold duty of an exporter under the EAR is to determine whether its product or technology is "subject to the EAR." As a general matter, all items exported from the United States are "subject to the EAR," and therefore within the scope of the EAR, except items subject to the jurisdiction of another export regime and publicly available technology or software.

With respect to items "subject to the EAR," the EAR control physical shipments out of the United States and technology transfers to foreign destinations and persons wherever located. The EAR also control re-exports of U.S.-origin items from locations outside of the United States; foreign made items containing more than a *de minimis* amount of U.S. components (defined as either 10% or 25% content depending upon the country); and, foreign made items that are the direct products of U.S.-origin technical data or software. The EAR also contains certain end-use prohibitions which implement U.S. foreign and national security policies, such as preventing weapons proliferation.

C. Commerce Control List and Country Chart

Items "subject to the EAR" include all items listed on the CCL and all other items meeting the definition of that term.[14] Generally, unless exclusively controlled for export or re-export under one of the other export regimes, e.g. the ITAR, items "subject to the EAR' include items in the United States, all U.S.-origin items wherever located, certain foreign-made commodities incorporating controlled U.S.-origin commodities, and certain foreign-made direct products of U.S. origin technology or software. Items "subject to the EAR" that are not listed on the CCL are designated as "EAR99."

The CCL is divided into ten (10) industry category groups on the CCL: [15]

(0) Nuclear Materials, Facilities and Equipment, and Miscellaneous;

(1) Materials, Chemicals, "Microorganisms," and Toxins;

(2) Materials Processing;

(3) Electronics Design, Development and Production;

(4) Computers;

(5) Telecommunications and Information Security;

(6) Sensors;

(7) Navigation and Avionics;

(8) Marine; and,

(9) Propulsion Systems, Space Vehicles, and Related Equipment.

Each of the ten category groups contains descriptions of items corresponding to a unique Export Classification Number ("ECCN"). The ECCN is an alphanumeric code that describes a particular item or type of item. Each ECCN listing sets forth various reasons for control which correspond to columns set forth in the Country Chart – a comprehensive list of country destinations. If the ECCN and Country Chart indicate that a reason for control applies to a particular country, items subject to that ECCN require a license for export to that country unless an exception is available.

D. General Prohibitions

1. Overview of the General Prohibitions

After determining that an item is "subject to the EAR," an exporter must assess how the EAR's ten (10) General Prohibitions apply to the export of that item. If one or more of the General Prohibitions applies, and no license exceptions may be used, then the exporter must seek a license from the Commerce Department. Only four General Prohibitions are subject to license exceptions.

Prohibitions One (1) through Three (3) relate to product controls and are subject to certain license exceptions. They are as follows:

- **Prohibition One:** Exports and Re-exports;
- **Prohibition Two:** U.S. Content Re-exports; and
- **Prohibition Three:** Foreign-Produced Direct Product Re-exports

General Prohibitions Four (4) through Ten (10) relate to activities that are prohibited without the express written permission of the BIS. Except for Prohibition Eight, these controls are ***not*** subject to license exceptions; licenses are required in ***all*** circumstances. These prohibitions are as follows:

- **Prohibition Four:** Denial Orders;
- **Prohibition Five:** End-Use/End-User;
- **Prohibition Six:** Embargo;
- **Prohibition Seven:** U.S. Person Proliferation Activity;
- **Prohibition Eight:** In transit;
- **Prohibition Nine**: Orders, Terms and Conditions; and
- **Prohibition Ten:** Knowledge Violation to Occur

2. Guide to Using the General Prohibitions

General Prohibition One: Exports and Re-exports

This Prohibition provides that you may not, without a license or license exception, export any item subject to the EAR to another country or re-export any item of U.S. origin if each of the following is true: (1) The item is controlled for a reason indicated in the applicable ECCN; and (2) export to the destination requires a license for the control reason as indicated on the Country Chart.

- How to Apply Prohibition One:
    - Classify your commodity/technology on the Commerce Control List ("CCL"). If you are not familiar with the technology, request assistance from someone who is.
    - Record the classification analysis in a memo and retain it in your files. If you do not personally make the classification, ask the person who did to write the file memo.
    - Does the ECCN entry show a license requirement? If yes, look up your destination country on the EAR's Country Chart (Part 738). Is a license required for **any** Reason for Control listed (an "X" will appear in the column under the Reason for Control).
    - Record whether a license is required and whether any license exceptions apply, and continue your review of the other Prohibitions.

General Prohibition Two: Parts and Components Re-exports

This Prohibition provides that you may not, without a license or license exception, re-export or export *from* abroad, any foreign-made commodity, software, or technology incorporating or bundled with U.S.-origin commodities, software, or technology that is controlled to the country of ultimate destination if the foreign-made item *meets all three* of the following conditions: (1) It incorporates more than a de minimis amount of controlled U.S. content (refer to EAR § 734.4 for de minimis rules); (2) it is controlled for a reason indicated in the applicable ECCN; and (3) export to the ultimate destination requires a license for that control reason, as indicated on the Country Chart.

- How to Apply Prohibition Two:
  - Determine if your item is foreign-made, review the EAR definition of "foreign made." If your item is not "foreign made," record this result for your files and continue with your examination of the other Prohibitions.
  - Is your item a foreign-made item that includes U.S.-origin components? If yes, then you must determine if the U.S.-origin content is more than de minimis, i.e., a small enough part of the whole that its export/re-export may not be prohibited by this Prohibition. The procedure for calculating the value of the U.S.-origin parts for this purpose is found at Supplement 2 of Part 734 of the EAR.
  - Keep a record of your calculations for your file. If this calculation shows that the U.S.-origin content is de minimis, then this Prohibition does not apply. Make a record of this result and continue your consideration of the other Prohibitions.
  - If the U.S.-origin content is more than de minimis, then look at the ECCN of the item you wish to export/re-export.
  - Does the ECCN entry show a license requirement? If so, look up your destination country on the Country Chart and see if a license is required for each Reason for Control listed (an "X" will appear in the column under the Reason for Control).
  - Record whether a license is required and any possible license exceptions. Continue your review of the other Prohibitions.

General Prohibition Three: Foreign-Produced Direct Product Re-exports

This Prohibition provides that you may not re-export or export from abroad foreign-made items subject to the scope of this General Prohibition to Cuba or any country in Country Group D:1 *(See* Supplement No. 1 to EAR Part 740). Foreign-made items are subject to this prohibition if they meet either of the following conditions:

- **Direct Product of Technology**. Foreign-made items are subject to this prohibition if both of the following criteria exist: (i) They are direct product of technology or software that requires a written assurance as a supporting document for a license or as a precondition for the use of License Exception TSR; and (ii) they are subject to national security controls as designated on the applicable ECCN.

- **Direct Product of a Plant.** Foreign-made items are subject to this prohibition if they are the direct product of a complete plant or any major component of a plant if both of the following criteria are present: (i) The plant or component is the direct product of technology that requires a written assurance as a supporting document for a license or as a precondition for the use of License Exception TSR; and (ii) the foreign-made products of the plant or component are subject to national security controls as designated on the applicable ECCN.

- How to Apply Prohibition Three:

    - Determine if your item is foreign-made. If not, then record this result and continue your consideration of the rest of the other Prohibitions.
    - If your item is foreign-made, is it the direct product of technology or software that requires a written assurance as a supporting document for a license or as a precondition for use of License Exception TSR?
    - Look up your item on the CCL. Does the ECCN for the item show that it is controlled for national security reasons? If the answer to this and the preceding question is "yes," then this prohibition applies. Record this result and continue with your consideration of the other Prohibitions.
    - Is your foreign-made item the direct product of a complete plant or major component of a plant? If not, then record this result and continue your consideration of the remaining prohibitions. If yes, is the plant or component the direct product of technology that requires a written assurance as a supporting document for a license or as a precondition for the use of License Exception TSR?
    - Look up your item on the CCL. Does the ECCN for the item show that it is controlled for national security reasons?
    - If the answer to the two preceding questions is "yes", then this prohibition applies and you are prohibited from transmitting the item to any country listed in Country Group D:1 (See Supplement No. 1 to Part 740 of the EAR).

- Record this result and continue with your consideration of the other prohibitions.

General Prohibition Four: Denial Orders

This Prohibition provides that you may not take any action that is prohibited by a denial order issued under EAR Part 766 (Administrative Enforcement Proceedings). These orders prohibit many actions in addition to direct exports by the person denied export privileges, including some transfers within a single country, either in the U.S. or abroad, by other persons. You are responsible for ensuring that none of your transactions involve a person who is subject to a denial order. Names of persons denied export privileges are published in the Federal Register and are also included on the Denied Persons List, located in Supplement 2 of EAR Part 764. There are ***no*** license exceptions that authorize conduct prohibited by this Prohibition.

- How to Apply Prohibition Four:
  - Check each person, company or entity involved in your transaction against the denied persons list.[16]
  - If the name appears, check the actual order and determine if its terms allow this party to be involved in your proposed transaction and how. Consult with company counsel or export compliance specialist when reviewing the order.
  - Record this result and continue your consideration of the other Prohibitions.

General Prohibition Five: End-Use/End-User

This Prohibition provides that you may not, without a license, knowingly export or re-export any item subject to the EAR to an end-user or end-use that is prohibited by EAR Part 744. EAR Part 744 places restrictions on certain nuclear end-uses, certain missile, chemical and biological weapons, and maritime nuclear propulsion end uses. Part 744 also restricts certain activities by U.S. persons, and certain exports to and for the use of certain foreign vessels or aircraft.

- How to Apply Prohibition Five:
  - Regardless of any other Prohibitions that may or may not apply, if your end-user is prohibited or the end-use of the item is against the nonproliferation policies of the United States, you may not complete your transaction. Therefore, you must review each end-use and end-user prohibition and determine if they are applicable to your transaction.
  - Review the BIS's "Know Your Customer" Guidance and Red Flags, which are found at Supplement 2 to Part 732 of the EAR.
  - If this Prohibition applies, record this result and continue your review of the other Prohibitions.

General Prohibition Six: Embargo

This Prohibition provides that you may not, without a license or license exception authorized under EAR Part 746, export or re-export any item subject to the EAR to a country that is embargoed by the U.S. or otherwise made subject to controls, as described in EAR Part 746. There are two categories of controls in Part 746 as follows:

- **Comprehensive controls.** Countries subject to general embargoes or special end-user controls currently include Cuba and Iran**.** Comprehensive embargoes to Cuba, Iran and other countries are also administered by the Department of Treasury's Office of Foreign Assets Control. Authorizations may be required from Treasury in addition to any Commerce Department authorization.

- **Sanctions on selected categories of items to specific destinations.** Certain designated countries are subject to controls on selected categories of items. These controls are in addition to those shown on the Country Chart.

- How to Apply Prohibition Six:

    - Because these controls extend to virtually all exports, they do not appear in the Country Chart or on the CCL.
    - If your destination is Cuba, you will almost definitely need a license and you will probably be denied.
    - If your destination is any country specified in Part 746 of the EAR, then consult the Company Export Compliance Specialist.
    - If Prohibition Six applies, record this result and continue your consideration of the other Prohibitions.

General Prohibition Seven: U.S. Person Proliferation Activity

This Prohibition provides that if you are a U.S. Person, you may not, without a license, engage in certain financing, contracting, service, support, transportation, freight forwarding or employment that you know will assist in proliferation activities described in EAR Part 744. EAR §§ 744.6(a) and (b) prohibit you from exporting, re-exporting, or transferring without a license any item where you know that the item will be used in the design, development, production or use of: (i) of nuclear explosive devices in or by a country listed in Country Group D:2 *(See* Supplement No. 1 to EAR Part 740); (ii) missiles in or by a country in Country Group D:4 (*See* Supplement No. 1 to EAR Part 740); or (iii) chemical or biological weapons in or by any country or destination worldwide.

This Prohibition also provides that if you are a U.S. Person you may not export (i) a Schedule 1 chemical listed in Supplement No. 1 to EAR Part 745 without first complying with the provisions of EAR §§ 742.18 and 745.1, or (ii) a Schedule 3 chemical listed in Supplement No. 1 to EAR Part

745 to a destination not listed in Supplement No. 2 to EAR Part 745 without complying with the End-Use Certificate requirements in EAR § 745.2 that apply to certain Schedule 3 chemicals.

- How to Apply Prohibition Seven:

  - Do you have any reason to believe that the item you wish to transmit will be used in any of the above three activities? This prohibition also applies to items not listed on the CCL or designated as EAR 99. If yes, you must apply for a license.
  - You must also apply for a license if you wish to support such a transaction, which includes financing, transportation, and freight forwarding (i.e., facilitating the export, re-export, or transfer without being the actual exporter/re-exporter).
  - You are also prohibited from a variety of activities that do not relate to exports. You may not: (i) perform any contract, service, or employment that you know will directly assist in the design, development, production, or use of missiles in or by a country listed in Country Group D:4; (ii) perform any contract, service, or employment that you know will directly assist in the design, development, production, stockpiling, or use of chemical or biological weapons in or by a country in Country Group D:3; and (iii) participate, without a license, in the design, construction, export, or re-export of a whole plant to make chemical weapons precursors identified in ECCN 1C350, in countries other than those listed in Country Group A:3.
  - If you are "informed" by BIS, either personally or by amendment of the EAR, that a license is required because an activity could involve the types of participation and support described above, you may not proceed with your transaction without obtaining a license from BIS. However, a license request will likely be denied.
  - If this Prohibition applies, record this result and continue your consideration of the other Prohibitions.

General Prohibition Eight: In-transit

This Prohibition provides that you may not export an item through or transit through any of the following countries unless authorized under a license or license exception, or unless such export or reexport is eligible to the country without a license:

Albania	Armenia	Azerbaijan	Belarus
Cambodia	Cuba	Georgia	Kazakhstan
Kyrgyzstan	Laos	Mongolia	North Korea
Russia	Tajikistan	Turkmenistan	Ukraine
Uzbekistan	Vietnam		

- How to Apply Prohibition Eight:
    - Determine the route your shipment will take to its ultimate destination.
    - If it is scheduled to pass through any of the above countries you must either (1) reroute it, or (2) determine if a license would be required if you were exporting your item/data to that country and if a license exception would apply.
    - If you would require a license to send the item to an end-user in the intermediate country, you must obtain the license before you ship.
    - If this Prohibition applies and you do not elect to have the shipment re-routed, you must repeat the analysis of your item under all ten Prohibitions using the intermediate country as the end destination.
    - Record whether this Prohibition applies and what decision you have made.

General Prohibition Nine: Orders, Terms, and Conditions

This Prohibition provides that you may not violate terms or conditions of a license or of a license exception issued under or made part of the EAR. You also may not violate any order issued under or made part of the EAR.

- How to Apply Prohibition Nine:
    - This Prohibition is self-explanatory. When you operate under a license, you are obligated to operate under **all** of its terms. When you use a license exception to obviate the need to apply for a license, you must qualify under **all** terms of the exception and you may not violate any of its conditions. You also may not violate any terms of any order.

General Prohibition Ten: Knowledge Violation to Occur

This Prohibition provides that you may not: (i) Sell, transfer, export, re-export, finance, order, buy, remove, conceal, store, use, loan, dispose of, transfer, transport, forward, or otherwise service, in whole or in part, any item subject to the EAR, exported or to be exported, with knowledge that a violation of the EAA, EAR or any order, any license, license exception, or other authorization has occurred, is about to occur, or is intended to occur in connection with the item; or (ii) rely on any license or license exception after notice to you of the suspension or revocation of that license or exception.

- How to Apply Prohibition Ten:
  - This Prohibition is also self-explanatory. You may not "blind" yourself to the reality that a violation is to occur. If you have any reason to know that a violation is to occur, you may not be involved in any aspect of the transaction. You also may not rely on a license or license exception after you have been notified that the license or the exception is no longer available for use.

E. Applying for a License

The EAR may require a license for items "subject to the EAR" (unless an exception applies) and it can prohibit other specified conduct related to export activities. If a license is required, the exporter must make application to BIS on Form BIS-748P, "Multipurpose Application Form." License application requirements are set forth at EAR Part 748. BIS maintains an online system for filing license applications and materials, known as the SNAP-R Electronic Licensing System, which can be found on the BIS website. If approved, the exporter will receive a license number and expiration date, which must be used on export documents. BIS licenses usually are valid for two years.

F. Dual Licensing Considerations

With respect to items shifting from the USML to the CCL pursuant to recent rules implemented under the ECR initiative, the Departments of State and Commerce have determined that a DTC license, agreement, or other approval received in accordance with ITAR regulation § 120.5(b) will also satisfy the BIS license requirement. Accordingly, under § 743.3(e), a BIS license will only be required when an export, re-export, or in-country transfer exceeds the scope of the DTC license, agreement, or other approval, or if it exceeds the scope of § 120.5(b).

G. NLR ("No License Required")

Most exports subject to the EAR will not require a license and will be eligible for export under the designation NLR - "No License Required." Provided that a General Prohibition does not apply, no

license is required when:

- The item is not specifically described on the CCL and is, accordingly, covered by the catch-all EAR99 classification; or
- The item is specifically described on the CCL but no control reason is "checked" on the Country Chart for that country of destination.

However, sanctions controls may override "no license required" treatment.

H. Note about *De Minimis*

The April 16, 2013, final rule issued by BIS as part of the ECR initiative creates a zero percent *de minimis* level for countries subject to an arms embargo. These countries will be listed in a new D:5 column to Country Group D. Items moved to the 600 series will still be subject to the same 25 percent *de minimis* level across the EAR for any item not being exported to a country subject to an arms embargo.

I. License Exceptions

Even if a license is required for a particular transaction, a License Exception may be available. A License Exception is a pre-approved authorization to export based on established conditions or criteria, all of which must be satisfied in order to use the exception. EAR Part 740 describes various license exceptions which authorize exports or re-exports under specific conditions when the item or technology would otherwise require a license under General Prohibitions One, Two, Three, or Eight.

The April 16, 2013, final rule altered certain license exceptions by adding new country groups and, in some cases, broadening the scope of license exceptions. The following license exceptions were altered:

- TMP (temporary imports, exports, reexports, and transfers): Stylistic changes.
- RPL (servicing and replacement of parts and equipment): Stylistic changes.
- GOV (governments, international organizations, and international inspections under the Chemical Weapons Convention, and International Space Station): The final rule expands GOV to authorize items consigned to non-governmental end users acting on behalf of the U.S. Government in certain situations, subject to written authorization from the appropriate agency and additional export clearance requirements. Additionally, the final rule expands the scope of countries eligible to receive items on the Sensitive List to include the governments of those 36 countries not listed in Country Group A:5.

- TSU (technology & software—unrestricted): The rule broadens the TSU license exception by including in the concept of "Operation Technology" training information that is necessary for the operation of the commodity or software lawfully exported or reexported under a license. The final rule also adds TSU authorization for the release of software source code and technology in the U.S. by U.S. universities to their bona fide and full-time regular foreign national employees.

- STA (strategic trade authorization): This new license exception is designed to facilitate transfers to low risk countries and to promote interoperability with allies in the field. It is important because the final rule authorizes a number of 600 series ".a - .w" and ".x" items for export without a license to 36 countries—found now in Country Group A:5 in Supplement No. 1 to part 740—if the items are for end use by a government of those countries. The 600 series item will need to be marked as eligible for export under STA to benefit from the license exception.

The final rule also created a new ECCN 9A610.a covering aircraft that are specially designed for a military use and that are not enumerated in the revised USML Category VIII(a).

J. Controls on Encryption Products and Technology

Encryption items are items having – or designed for the production, development or use of – any encryption, decryption, and/or key management functionality. The EAR controls encryption items in a way which is much different from other items subject to the EAR. Although encryption controls have been revised and to some extent simplified over the years, they remain complex. As with technology generally, an "export" of an encryption item under the EAR is not just the physical shipment across borders of a production containing such functionality. An "export" also occurs when encryption technology is released to a foreign national or when encryption software is made available for transfer to persons outside the U.S. by any means of communication – including posting on a website.

U.S. encryption controls rest on three principles: (i) Review of encryption items before their sale; (ii) certain notification obligations; and (iii) license review for the export and re-export of particularly strong encryption items. Most encryption items, whether "mass market" products or not, are subject to a license exception that permits export following a 30-day review period, whether intended for export to government or non-government end-users. Reviews are conducted by BIS.

For exports to some designated countries, including the nations of the European Union, exports can occur immediately following submission of the review request. Also, review is not generally required for encryption items exported or re-exported to U.S. companies and their subsidiaries in any country except several specified, highly-controlled destinations, for internal company use including for new product development.

K. Antiboycott Controls

The EAR also prohibits participation in boycotts or restrictive trade practices that are not supported by the United States. The regulations impose reporting requirements on entities who receive any requests by third parties to participate in such activities. Reports must be filed with BIS detailing the request received. Details must include the nature of the request, the entity or person requesting participation in boycotting activities, the type of documents in which the request was received, and the response, if any, provided by the company receiving the request.

U.S. entities or persons subject to the jurisdiction of the United States may not respond to any request to participate in boycotting activities, whether the request seeks active participation in the boycott (e.g., a request that the party refuse to do business with the boycotted country or nationals of a boycotted country), or passive participation (e.g., a request to furnish information about business relationships with a boycotted country or its nationals).

The regulations also require companies to maintain records related to antiboycott activities for a period of five (5) years. Violations of the antiboycott regulations are punishable by substantial civil penalties.

Countries which have been the source of boycott requests include:

Bahrain	Oman	United Arab Emirates
Kuwait	Qatar	Yemen
Lebanon	Saudi Arabia	

1. Prohibited Actions in Furtherance of a Boycott

The antiboycott regulations identify specific actions which U.S. entities subject to U.S. jurisdiction may not pursue. No licenses may be obtained to participate in any of the prohibited activities. The regulations specifically prohibit agreements to:

- Refuse to, or actual refusals to, do business with or in a boycotted or blacklisted country or with nationals or residents of a boycotted country;
- Discriminate, or actual discrimination, against other persons based on race, religion, sex, national origin, or nationality;
- Furnish, or actually furnishing information, about business relationships with or in boycotted countries or blacklisted companies;
- Furnish, or actually furnishing information, about the race, religion, sex, or national origin of another person;

- Furnish, or actually furnishing information, about business relationships with blacklisted companies or with blacklisted persons;
- Furnish, or actually furnishing information, about associations with charitable and fraternal organizations; and
- Implement letters of credit containing prohibited boycott terms or conditions.

2. Identifying Boycott Requests

A "boycott request" can take many forms, such as requests to supply information or to take or refrain from action. Requests can be made during negotiations or can be "imbedded" in bid invitations, proposed contracts, purchase orders, letters of credit or other agreements, or requirements to provide information or to take or refrain from some action. Information obtained on one's own initiative from exporter guidebooks or other general sources is not considered to have been "requested." But, if such materials are provided by another party with instructions to observe the requirements therein (or "to do what is necessary") in connection with a transaction, a request has been received. Any request, condition, direction, or contract provision which contains the words "boycott" or "blacklist," or any reference to Israel, Israeli goods, Israeli nationals, Jews or Jewish organizations, should be considered a boycott request. Boycott requests should be presumed to be reportable, although exceptions do exist.

The following are typical examples of boycott requests:

- **Boycott Questionnaires.** Requests from boycott offices in Arab countries or other government authorities seeking information about a company's relationships with or investment in Israel or particular firms or persons, including data about the company's ownership, management, subsidiaries, licensees, and affiliates.
- **Requests for Negative Country-of-Origin Information.** Requests from foreign customs or import authorities or consulates or chambers of commerce, or provisions in contracts or letters of credit, seeking confirmation (often in the form of a certification or documentary endorsement) that the goods or services are not of Israeli origin, do not contain any Israeli-origin parts or materials, or were not produced by an Israeli firm or with Israeli labor or capital.
- **Requests for Negative Carrier/Insurance/Supplier Blacklisting Information.** Requests from foreign customs or import authorities or consulates or chambers of commerce, or provisions in contracts or letters of credit, seeking confirmation (often in the form of a certification or documentary endorsement) that the supplier, foreign insurer, vessel, or others are not "blacklisted."
- **Requests for National Origin, Nationality, Religious Affiliation Information.** Requests from government agencies or contractors for information about the religion, national origin, or charitable or fraternal association of persons in the management or employment of a firm (except request from immigration authorities or embassies or

consulates directed to a particular individual about himself for his own response as part of the visa process), and provisions excluding persons of the Jewish faith or of Israeli national origin or nationality.

- **Requests to Exclude Blacklisted Firms.** Requests from contractors or consulting firms to select a particular supplier or subcontractor, if there is knowledge or reason to know that blacklisted firms have been excluded in the selection process; or not to select a particular supplier or subcontractor known or believed to be blacklisted; or to select from among a group of suppliers or subcontractors from which blacklisted firms have been excluded.

- **Requests to Comply with Boycott Requirements.** Clauses in contracts or tender documents which require the firm doing business with an Arab country or customer to comply generally with the local boycott law or regulations or practices or with specific boycott requirements; or clauses which make any of such laws, regulations, or practices applicable to performance of the contract.

- **Boycott-Related Terms or Conditions.** Terms or conditions from customers or government authorities or others in import permits (e.g., not negotiable in Israel) or letters of credit or packaging instructions (e.g., non-use of six-pointed stars) or shipping document instructions (e.g., Israeli certificate of origin not acceptable) the effect of which is to preclude dealings with Israeli or blacklisted firms.

3. Withholding Responsive Actions

No action responsive to any Arab boycott request should be taken without the express advance approval of a responsible compliance manager. Any action, including the furnishing of information, could be considered responsive to the request if it has the effect of:

- Providing the information sought;

- Ensuring that the action sought to be accomplished will be or has been taken;

- Ensuring that the action sought to be prevented has not been or will not be taken; or

- Ensuring that the agreement or undertaking sought has been or will be given.

Where a boycott specification or term in a contract, purchase order, letter of credit, or other document calls for taking a prescribed action — e.g., not using a blacklisted carrier or supplier — that specification or term should not be ignored. The transaction should not go forward until the objectionable specification has been effectively eliminated from the contract or other document.

Actions not requested — but if requested, might be prohibited — also should not be taken without the express advance approval of a responsible compliance manager. For example, a recipient

should not provide a negative certificate of product origin or a non-blacklisted confirmation, whether or not requested to do so.

4. Limiting Exposure from Third Parties

The actions of agents, consultants, advisors, partners, co-venturers, and others having a contractual relationship with a company, which gives those third parties the potential ability to act on behalf of the company, may create exposure for the company. Accordingly, such third parties need to be aware of the company's obligations under the anti-boycott law. As part of a company's internal compliance program, a review should be made of all company contract documents. Where necessary, contracts should contain provisions designed to reduce the risk to the company that these parties might take action that would expose the company to liability, including the express requirement of prior approval of a responsible compliance manager before specified actions are taken.

5. Other International Boycotts

U.S. antiboycott laws also apply to other international economic boycotts directed to countries friendly to the U.S. Requests for information, action, or agreements indicating the existence of any "international boycott" should be assessed before responding.

M. Definitions of Key EAR Terms

Part 772 of the EAR contains the majority of the definitions applicable to dual-use exports. Some, but by no means all, of the definitions of important terms follow. Definitions for all of the terms below can also be found at EAR § 772.1, or in other sections of the EAR as indicated.

The April 16, 2013, final rule issued pursuant to the ECR initiative changed a number of definitions, and added definitions that were not previously included in the EAR. Some of the definitions added to the EAR are now included in both the EAR and the USML.

1. Applicant

The person who applies for an export or re-export license, and who has the authority to determine and control the export or re-export of items.

2. Category

The Commerce Control List ("CCL") is divided into ten (10) categories: (0) Nuclear Materials, Facilities and Equipment, and Miscellaneous; (1) Materials, Chemicals, "Microorganisms," and Toxins; (2) Materials Processing; (3) Electronics Design, Development and Production; (4) Computers; (5) Telecommunications and Information Security; (6) Sensors; (7) Navigation and Avionics; (8) Marine; and (9) Propulsion Systems, Space Vehicles and Related Equipment.

3. Commerce Control List

A list of items under the export control jurisdiction of the Bureau of Industry & Security, U. S. Department of Commerce. (*See* EAR Part 774).

4. Commodity

Any article, material, or supply except technology and software. Note that the provisions of the EAR applicable to the control of software (e.g., publicly available provisions) are not applicable to encryption software. Encryption software is controlled because it has a functional capacity to encrypt information on a computer system, and not because of any informational or theoretical value that such software may reflect, contain or represent, or that its export may convey to others abroad.

5. Countries Supporting International Terrorism

The Secretary of State has determined that certain countries' governments have repeatedly provided support for acts of international terrorism, such as Cuba, Iran, North Korea, Sudan and Syria.

6. Country Chart

A chart, found in Supplement No. 1 to EAR Part 738, containing certain licensing requirements based on destination and reason for control. In combination with the Commodity Control List ("CCL"), the Country Chart indicates when a license is required for any item on the CCL sent to any country in the world under Prohibition One (Exports and Re-exports in the Form Received), Prohibition Two (Parts and Components Re-exports), and Prohibition Three (Foreign Produced Direct Product Re-exports).

7. Country Groups

For export control purposes, foreign countries are separated into five country groups designated by the symbols A, B, C, D, and E. (*See* Supplement No. 1 to EAR Part 740 for lists of countries in each Country Group). The April 16, 2013, final rule issued pursuant to the ECR initiative adds two new columns to Country Group A, which incorporate the lists of countries previously set forth in the text of License Exception STA. The final rule also adds one new column to Country Group D, which incorporates the list of countries subject to the U.S. arms embargo.

8. Designed or Modified

Equipment, parts, components, or "software" that have, as a result of "development" or modification, specified properties that make them fit for a particular application. "Designed or modified" equipment, parts, components, or "software" can be used for other applications. Used in the Missile Technology Control Regime ("MTCR") context.

9. Development

"Development" is related to all stages prior to serial production, such as: design, design research, design analysis, design concepts, assembly and testing of prototypes, pilot production schemes, design data, process of transforming design data into a product, configuration design, integration design, and layouts. (*See* General Technology Note, Supplement No. 2 to EAR Part 774).

10. Dual Use

This term refers to items having both commercial and military, or proliferation, applications. While this term is used informally to describe items that are subject to the EAR, purely commercial items are also subject to the EAR (*see* § 734.2(a) of the EAR).

11. Encryption Component

Any encryption commodity or software (except source code), including encryption chips, integrated circuits, application specific encryption toolkits, or executable or linkable modules that alone are incapable of performing complete cryptographic functions, and is designed or intended for use in or the production of another encryption item.

12. Encryption Items

The phrase "encryption items" includes all encryption commodities, software, and technology that contain encryption features and are subject to the EAR. This does not include encryption items specifically designed, developed, configured, adapted, or modified for military applications (including command, control and intelligence applications) which are controlled under the ITAR.

13. Encryption Licensing Arrangement

A license that allows the export of specified products to specified destinations in unlimited quantities. In certain cases, exports are limited to specified end-users. Generally requires the exporter to meet certain reporting requirements.

14. Encryption Object Code

Computer programs containing encryption source code compiled into a form of code that can be directly executed by a computer to perform an encryption function.

15. Encryption Software

Computer programs that provide the capability of encryption functions, or confidentiality of information or information systems. Such software includes source code, object code, applications software, or system software.

16. Encryption Source Code

A precise set of operating instructions to a computer that, when compiled, allows for the execution of an encryption function on a computer.

17. End-User

The person abroad receiving and ultimately using the exported or re-exported items. Not a forwarding agent or intermediary, "end-user may be a purchaser or ultimate consignee."

18. Export

Export means an actual shipment or transmission of items out of the United States. *(See also* EAR § 734.2(b) which expands on the Part 772 definition of "export" to include the release of technology or software subject to the EAR to a foreign national wherever s/he is located).

19. Export Control Classification Number ("ECCN")

The numbers used in Supplement No. 1 to EAR Part 774 and throughout the EAR. The Export Control Classification Number consists of a set of digits and a letter. Reference EAR § 738.2 for a complete description of the composition of the ECCN.

20. Exporter

The person in the United States who has the authority of a principal party in interest to determine and control the sending of items out of the United States. Note that the Foreign Trade Statistics Regulations ("FTSR") have a different definition for the term "exporter." Under the FTSR, the "exporter" is the U.S. principal party in interest, e.g., the U.S. selling party who receives the primary benefit, monetary or otherwise, from the transaction as opposed to the forwarding or other agent *(See* FTSR, Title 15 part 30).

21. Firm

A corporation, partnership, limited partnership, association, company, trust, or any other kind of organization or body corporate, situated, residing, or doing business in the United States or any foreign country, including any government or agency thereof.

22. Foreign Government Agency

For the purposes of exemption from support documentation *(see* EAR § 748.9), a foreign government agency is defined as follows: (a) National governmental departments operated by government-paid personnel performing governmental administrative functions; e.g., Finance Ministry, Ministry of Defense, Ministry of Health, etc. (municipal or other local government entities must submit required support documentation); or (b) National government-owned public service entities; e.g., nationally owned railway, postal, telephone, telegraph, broadcasting, and

power systems, etc. The term "foreign government agency" does not include government corporations, quasi-government agencies, and state enterprises engaged in commercial, industrial, and manufacturing activities, such as petroleum refineries, mines, steel mills, retail stores, automobile manufacturing plants, airlines, or steamship lines operating between two or more countries, etc.

23. General Prohibitions

The ten (10) prohibitions found in part 736 of the EAR that prohibit certain exports, re-exports, and other conduct, subject to the EAR, absent a license, license exception, or determination that no license is required ("NLR").

24. Intermediate Consignee

The person acting as an agent for a principal party in interest for the purpose of effecting delivery of items to the ultimate consignee. The intermediate consignee may be a bank, forwarding agent, or other person who acts as an agent for a principal party in interest.

25. Item

Item means commodities, software, and technology.

26. Knowledge

Knowledge of a circumstance includes "reason to know" or "reason to believe." Knowledge includes not only positive knowledge that a circumstance exists or is substantially certain to occur, but also an awareness of a high probability of its existence or future occurrence. Such awareness can be inferred from evidence of the conscious disregard of facts known to a person and a person's willful avoidance of facts. This definition does not apply to EAR Part 760 (Restrictive Trade Practices or Boycotts).

27. License

Authority issued by BIS authorizing an export, re-export, or other regulated activity. The term "license" does not include authority represented by a "License Exception."

28. Licensee

The person to whom a license has been issued by BIS.

29. License Exception

An authorization described in Part 740 of the EAR that allows an export or re-export, under stated conditions, of items subject to the EAR that otherwise would require a license. Unless otherwise

indicated, license exceptions are not applicable to exports under the licensing jurisdiction of agencies other than the Department of Commerce.

30. Object Code or Object Language

An equipment-executable form of a convenient expression of one or more processes (source code or source language) that has been converted by a programming system. *(See also* "source code").

31. Open Cryptographic Interface

A mechanism designed to allow a customer or other party to insert cryptographic functionality without the intervention, help or assistance of the manufacturer or its agents, e.g., manufacturer's signing of cryptographic code or proprietary interfaces. If the cryptographic interface implements a fixed set of algorithms, key lengths, or key exchange management systems, that cannot be changed, it will not be considered an "open" cryptographic interface. All general application programming interfaces (e.g., those that accept either a cryptographic or non-cryptographic interface but do not themselves maintain any cryptographic functionality) will not be considered "open" cryptographic interfaces.

32. Person

A natural person, including a citizen or national of the United States or of any foreign country; any firm; any government, government agency, government department, or government commission; any labor union; and fraternal or social organization; and any other association or organization whether or not organized for profit. This definition does not apply to Part 760 of the EAR (Restrictive Trade Practices or Boycotts).

33. Production

Means all production stages such as product engineering, manufacture, integration, assembly (mounting), inspection, testing, and quality assurance (applies to General Technology Note).

34. Production Equipment

Tooling, templates, jigs, mandrels, moulds, dies, fixtures, alignment mechanisms, test equipment, other machinery, and components therefore, limited to those specially designed or modified for "development" or for one or more phases of "production" (applies in MTCR context).

35. Publicly Available Information

Information that is generally accessible to the interested public in any form and, therefore, not subject to the EAR. *(See* Part 732 of the EAR). Publicly available information includes fundamental research as defined in EAR Part 734.8, and educational information as defined in EAR Part 734.9.

36. Publicly Available Technology and Software

Technology and software that are already published or will be published; arise during, or result from fundamental research; are educational; or are included in certain patent applications. *(See* EAR § 734.3(b)(3)).

37. Purchaser

The person abroad who has entered into a transaction to purchase an item for delivery to the ultimate consignee. In most cases, the purchaser is not a bank, forwarding agent, or intermediary. The purchaser and ultimate consignee may be the same entity.

38. Reasons for Control

The reasons for control are: Anti-Terrorism (AT); Chemical and Biological Weapons (CB); Crime Control (CC); High Performance Computer (XP); Missile Technology (MT); National Security (NS); Nuclear Nonproliferation (NP); Regional Stability (RS); Short Supply (SS); and United Nations Sanctions (UN). Items controlled within a particular ECCN may be controlled for more than one reason.

39. Re-export

Re-export means an actual shipment or transmission of items subject to the EAR from one foreign country to another foreign country. For purposes of the EAR, the export or re-export of items subject to the EAR that will transit through a country or countries, or be transshipped in a country or countries to a new country, or are intended for re-export to the new country, are deemed to be exports to the new country. *(See* EAR § 734.2(b)). In addition, for purposes of satellites controlled by the Department of Commerce, the term re-export also includes the transfer of registration of a satellite or operational control over a satellite from a party resident in one country to a party resident in another country.

40. Required

As applied to technology or software, refers to only that portion of technology or software which is peculiarly responsible for achieving or extending the controlled performance levels, characteristics, or functions. Such required technology or software may be shared by different products.

41. Return without Action ("RWA")

An application may be "RWA'd" for one of the following reasons:

- The applicant has requested the application be returned;
- A license exception applies;

- The items are not under Department of Commerce jurisdiction;
- Required documentation has not been submitted with the application; or
- The applicant cannot be reached after several attempts to request additional information necessary for processing of the application.

42. Robot

A manipulation mechanism which may be of the continuous path or of the point-to-point variety, may use "sensors," and has all of the characteristics specified in ECCN Categories 2 and 8.

43. Schedule B Numbers

The commodity numbers appearing in the current edition of the Bureau of Census publication, Schedule B Statistical Classification of Domestic and Foreign Commodities Exported from the United States. (*See* EAR Part 758).

44. Software

A collection of one or more programs or microprograms fixed in a tangible medium of expression.

45. Source Code or Source Language

A convenient expression of one or more processes that may be turned by a programming system into equipment executable form (object code or object language).

46. Space Qualified

Products designed, manufactured, and tested to meet the special electrical, mechanical, or environmental requirements for use in the launch and deployment of satellites or high-altitude flight systems operating at altitudes of 100 Km or higher.

47. Specially Designed

Equipment, parts, components, or software that, as a result of development, have unique properties that distinguish them for certain predetermined purposes. For example, a piece of equipment that is specially designed for use in a missile will only be considered to be so if it has no other function or use. Similarly, a piece of manufacturing equipment that is specially designed to produce a certain type of component will only be considered such if it is not capable of producing other types of components (Applies to a MTCR context).

As a result of the ECR initiative changes announced on April 16, 2013, the definition of "specially designed" now incorporates a two-part "catch-and-release" approach intended to facilitate the

transition of items from the USML to the CCL. If an item is "caught" in section (a) (15 CFR § 772.1(a)) because it meets the criteria specified in that section, then it will be deemed "specially designed" for a military application unless it is "released" from that designation by application of the protocol in section (b) (15 CFR § 772.1(b)), which sets forth circumstances under which an item will not be considered "specially designed" for a military application. Any item "released" under section (b) would be classified elsewhere on the CCL or as EAR99, but not in subparagraph ".x" or ".y." subcategories of the 600 Series.

48. Subject to the EAR

A term used in the EAR to describe commodities, software, technology, and activities over which BIS exercises regulatory jurisdiction under the EAR. *(See* EAR § 734.2(a)).

49. Technical Assistance

A form of "technology" such as instruction, skills training, working knowledge, or consulting services. Technical assistance involves transfer of technical data.

50. Technical Data

May take forms such as blueprints, plans, diagrams, models, formulae, tables, engineering designs and specifications, manuals, and instructions written or recorded on other media or devices such as disk, tape, and read-only memories.

51. Technology

Specific information necessary for the development, production, or use of a product. The information takes the form of technical data or technical assistance. Controlled technology is defined in the General Technology Note and in the Commerce Control List.

52. Transfer

A transfer to any person of items subject to the EAR either within or outside of the United States.

53. Ultimate Consignee

The principal party in interest located abroad who receives the exported or re-exported items. Not a forwarding agent or other intermediary, the ultimate consignee may be the end-user.

54. United States

Unless otherwise stated, the 50 States, including offshore areas within their jurisdiction pursuant to section 3 of the Submerged Lands Act (43 U.S.C. § 1311), the District of Columbia, Puerto Rico, and all territories, dependencies, and possessions of the United States, including foreign trade

zones established pursuant to 19 U.S.C. 81A-81U, and also including the outer continental shelf, as defined in section 2(a) of the Outer Continental Shelf Lands Act (43 U.S.C. §1331(a)).

55. U.S. Person

As used throughout the EAR, the term "U.S. person" includes: any individual who is a citizen of the United States, a permanent resident alien of the United States, or a protected individual as defined by 8 U.S.C. § 1324b(a)(3); any juridical person organized under the laws of the United States or any jurisdiction within the United States, including foreign branches; and any person in the United States. (*See also* Parts 740.9 and 740.14 and Parts 746 and 760 of the EAR for definitions of U.S. Person that are specific to those parts).

56. Use

Means operation, installation (including on-site installation), maintenance (checking), repair, overhaul, and refurbishing.

VI. International Traffic in Arms Regulations

A. The ECR Initiative and the ITAR

The DTC final rule published on April 16, 2013, along with BIS' rule updates several USML categories and ITAR definitions. In addition, the DTC final rule sets forth a "Transition Plan" describing procedures for the shifting of articles from the USML to the CCL. The DTC final rule also created a new licensing procedure for exporting items subject to the EAR that are to be exported with defense articles.

1. Revised Categories

DTC's final rule revised USML Category VIII (Aircraft and Related Articles), Category XVII (Classified Articles, Technical Data, and Defense Services Not Otherwise Enumerated), and Category XXI (Articles, Technical Data, and Defense Services Not Otherwise Enumerated); and, created USML Category XIX (Gas Turbines Engines and Associated Equipment). A summary of these changes follows:

- **Category VIII**: Narrows the types of aircraft and related articles controlled under Category VIII to only those that warrant control under the requirements of the Arms Export Control Act ("AECA"). All parts, components, accessories, attachments, and equipment specially designed for the B-1B, B-2, F-15SE, F/A-18 E/F/G, F-22, F-35 or F-117, or U.S. Government technology demonstrators will remain in Category VIII.
- **Category XVII:** Makes stylistic changes only.

- **Category XIX:** Creates a new category that covers gas turbine engines and associated items. The new Category XIX supersedes the current controls on certain items under USML Categories IV, VI, and VII.

- **Category XXI:** Updates the language of Category XXI, clarify that any article not enumerated on the USML may be included in Category XXI until such time as the appropriate USML category is amended.

In another rule published on July 8, 2013, DTC revised USML Category VI (Surface Vessels of War and Special Naval Equipment), Category VII (Ground Vehicles), Category XIII (Materials and Miscellaneous Articles), and Category XX (Submersible Vessels and Related Articles). These revisions now more accurately describe the articles covered by each category, establishing a clearer line between the USML and the CCL.

2. Transition Plan

The Transition Plan sets forth (1) the timelines for implementation of changes to the USML, (2) temporary licensing procedures for items transitioning from the USML to the CCL, and (3) permanent licensing procedures pertaining to the export of any item "subject to the EAR." A summary of the Transition Plan follows:

- The Transition Plan provides a 180-day transition period between publication of the corresponding final rule for each revised USML category and the effective date of the transition to the CCL for items that will undergo a change in export jurisdiction.

- A license or authorization issued by the DTC will be effective for up to two years from the effective date of the revised USML category if all the items listed on the license or authorization have transitioned to the export jurisdiction of the U.S. Department of Commerce. A license or authorization issued by DTC will be valid until its expiration if some of the items listed on the license or authorization have transitioned to the export jurisdiction of the U.S. Department of Commerce.

- If a licensee is unsure of the proper ECCN designation for a USML article that has shifted to the CCL, it should submit a Commodity Classification Automated Tracking System request ("CCATS") to the U.S. Department of Commerce for an official and exclusive decision.

- USML categories will have a new "(x) paragraph," which will allow for ITAR licensing for commodities, software, and technical data subject to the EAR, provided that those commodities, software, and technical data are to be used in or with defense articles controlled on the USML and are described in the purchase.

3. Reexport/Retransfer of USML Items that have Transitioned to the CCL

Foreign persons who receive, via a U.S. Department of State authorization, an item that has transitioned to the CCL (e.g., confirmed in writing by manufacturer or supplier), should treat the item as such and submit requests for post-transition re-exports or retransfers to the U.S. Department of Commerce.

B. Registering under the ITAR

The ITAR is unlike the EAR in that, in addition to licensing, recordkeeping, and reporting requirements, an exporter, manufacturer or broker[17] of defense articles, technology, or services must first register with DTC, the agency charged with enforcing the ITAR. Manufacturers of defense articles are required to register whether or not they actually export defense articles. Registration is not a license to export; an exporter subject to the ITAR who has properly registered with DTC must still obtain license approval for the export of articles, technology, or technical services. DTC registration must be renewed annually at a fee varying with the volume of anticipated exports.

An intended registrant must complete and submit a Statement of Registration (Form DS-2032) with the required registration fee. The Statement of Registration must include a variety of information regarding the intended registrant, including: Its form of organization; its directors (including citizenship and identifying information); the Munitions List articles or services involved in the exporting, manufacturing, or brokering; and, information regarding U.S. and foreign subsidiaries and affiliates participating in the covered activities,

In addition, certifications must be included in the Statement of Registration as to whether the intended registrant, its officials and senior management, or members of the board of directors have previously been indicted or convicted of violating various U.S. criminal statutes enumerated in 22 C.F.R. Section 120.27, or are ineligible to contract with or receive an export or import license from, any U.S. Government agency. Registrations must be renewed annually. It is advisable to ask these certification questions of senior officials and board members at the same time the basic Statement of Registration information is gathered from them to minimize demands on their time.

Any material changes that occur over time to the information contained in the Statement of Registration must be reported to DTC by the registrant within five days of the effective date of the change. A material change includes: Changes to ineligibility information; changes to name, address, or senior officers/directors; establishment, acquisition, or divestment of a U.S. or foreign parent, subsidiary, or affiliate; a merger; or, addition or deletion of Munitions List categories. In addition, a registrant must notify DTC sixty days in advance of an intended sale or transfer to a foreign person of ownership or control of the registrant or any entity thereof. It should be noted that a filing with the Committee on Foreign Investment in the United States does not satisfy the ITAR sixty-day pre-notification requirement.

Registrants who determine that all of their activities involve articles or services that will transition from the USML to the CCL pursuant to the ECR initiative, and who are therefore no longer required to register with the U.S. Department of State, must provide written notification to the Department of State. Instructions for providing notification are accessible on the DTC website at

www.pmdtc.state.gov. The DTC will allow registrations to expire, but registrants must have maintained active registration until October 15.

C. Defense Articles and Defense Services

All exports of defense articles, defense services and technology related to defense articles must be licensed *prior* to export, unless one of the limited available exceptions under the ITAR applies.

1. Defense Articles

A "defense article" is defined as "any item or technical data designated in § 121.1 of this subchapter [ITAR]."[18] Section 121.1 is the United States Munitions List ("USML"). Items are listed on the USML because they:

- Are specifically designed, developed, configured, adapted, or modified for military application;
- Have a significant military or intelligence application;
- Do not have a predominant civil application; and
- Do not have performance equivalent, (i.e., form, fit and function, to items with a civil application).

In addition, even if an item is not specifically listed on the USML, it will nonetheless be viewed as a "defense article" if it is specially designed, developed, configured, adapted, or modified for a military application and it has significant military or intelligence applications justifying control as a "defense article." DTC possesses substantial discretion with respect to these determinations.

Following publication of the DTC and BIS final rules on April 16, 2013, pursuant to the ECR initiative, the ITAR definition of "specially designed," like the EAR definition, now includes a "catch" and "release" protocol. That protocol only applies to revised categories, however, and does not replace the phrase or meaning of "specifically designed" as currently used in the ITAR and USML.

Except for certain described commodities or software, a commodity or software (*see* ITAR § 121.8(f)) is "specially designed" if it:

- As a result of development, has properties peculiarly responsible for achieving or exceeding the controlled performance levels, characteristics, or functions described in the relevant USML paragraph; or
- Is a part, component, accessory, attachment, or software for use in or with a defense article.

A part, component, accessory, attachment, or software is not controlled by a USML "catch-all" or technical data control paragraph if it:

- Is subject to the EAR pursuant to a commodity jurisdiction determination;
- Is, regardless of form or fit, a fastener (e.g., screws, bolts, nuts, nut plates, studs, inserts, clips, rivets, pins), washer, spacer, insulator, grommet, bushing, spring, wire, or solder;
- Has the same function, performance capabilities, and the same or "equivalent" form and fit as a commodity or software used in or with a commodity that: (i) Is or was in production (i.e., not in development); and (ii) is not enumerated on the USML;
- Was or is being developed with knowledge that it is or would be for use in or with both defense articles enumerated on the USML and also commodities not on the USML; or
- Was or is being developed as a general purpose commodity or software, i.e., with no knowledge for use in or with a particular commodity (e.g., F/A-18 or HMMWV) or type of commodity (e.g., an aircraft or machine tool).

If an exporter is uncertain about whether a particular article is "specially designed" for a military application, it should submit a Commodity Jurisdiction Request.

"Technical data," also viewed as a "defense article," is broadly defined to include:

- Information, other than software, required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles;
- Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-series items controlled by the Commerce Control List;
- Information covered by an invention secrecy order; and
- Software as defined in § 121.8(f) directly related to defense articles.

Technical data can take many forms, such as:

- Blueprints;
- Drawings;
- Photographs;
- Computer software; and

- Documentation.

Technical data does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges and universities or information in the public domain as defined in § 120.11. It also does not include basic marketing information on function or purpose or general system descriptions of defense articles.

2. Defense Services

As noted, the ITAR control not only the export of defense articles, but also defense services directly related to articles enumerated in the USML. A "defense service" is defined as "[t]he furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles," or "the furnishing to foreign persons of any technical data controlled under this subchapter ... whether in the United States or abroad." [19]

D. Licenses and Agreements

Under the ITAR, a license must be obtained for the export of articles, technology, technical data, or technical services controlled on the USML prior to shipment or transfer. The process includes completing an export license application, researching the *bona fides* of the end-user, confirming the use to which the export will be put, and submitting certifications regarding the method through which the business was obtained. DDTC will issue a license, with any limitations appended ("provisos"), valid for a specified period of time (e.g., 24 months, 48 months). An exporter must maintain export records for a minimum of five years in a manner readily accessible to the U.S. Government for review.

A variety of types of licenses and authorizations are issued pursuant to the ITAR. DTC maintains a fully electronic system for licensing, called "D-Trade", which can be accessed on its website. At the present time, processing of only some types of license requests can be done on D-Trade.

1. Equipment Exports

Equipment listed on the USML or otherwise designated as a "defense article" may be exported only pursuant to an approved license; this requirement applies to both permanent and temporary exports of "defense articles." Exemptions are available, subject to clearance and other requirements, permitting "defense article" exports:

- Pursuant to technical assistance, manufacturing license, distribution or comprehensive agreements, without separate licensing of the "defense articles" if explicitly authorized under the agreement;

- On a temporary basis for such purposes as trade shows, public exhibitions, etc.;

- Such as components, parts, tools, and test equipment on a temporary basis to a subsidiary, affiliate, or facility owned or controlled by the U.S. exporter;
- Exported by or for U.S. Government agencies; or
- Exported pursuant to a Department of Defense ("DoD") Letter of Offer and Acceptance issued under the Foreign Military Sales program.

2. Technical Data Transfers

Permanent and temporary exports of technical data relating to "defense articles" or "defense services" must be licensed unless the technical data is beyond the scope of the ITAR or an exemption applies.

Like the EAR, technical data which is in the public domain because it is published and generally accessible or available to the public is beyond the scope of the ITAR. Information is considered in the public domain when it is generally accessible or available to the public through: (i) Sales at newsstands and bookstores, subscriptions available without restriction, distribution at conferences open to the public, any patent office, and libraries accessible by the public; or (ii) public release or unlimited distribution, following approval of a sponsoring agency. However, whereas the EAR contemplates that information can be proactively placed in the public domain by simply making it publicly available, the ITAR in contrast contemplates prior government review and approval before making information publicly available.

Technical data exports are exempt from licensing requirements when:

- Disclosed pursuant to DoD directive or the authorization of a cognizant U.S. Government sponsor;
- Approved for export pursuant to a technical assistance, manufacturing, distribution, or comprehensive agreement;
- Exported in furtherance of a U.S. government contract providing for such export (except that this exemption does not apply to design, development, production, or manufacturing technology);
- Previously authorized for export by the same exporter in the exact same form;
- Operations, maintenance and training information relating to equipment subject to an export license;
- Relating to small firearms;
- Being returned to the original foreign source in the same form;
- Related to classified data licensed for export to the same recipient;

- Being sent to a U.S. citizen employee of the exporter or of a Government agency for their use abroad;
- Exported by institutions of higher learning under limited circumstances; or
- Exported to nationals of National Atlantic Treaty Organization ("NATO") and specified other allies in order to respond to a written request from the DoD for a quote or proposal.

Use of exemptions is subject to specified shipping clearance and other requirements.

3. Agreements

The ITAR provide various licensing authorizations in the form of "agreements" to accommodate exports of "defense articles" and "defense services" during performance of commercial teaming, licensing, joint venture, and distribution agreements between U.S. companies and foreign partners. The agreements are entered into by and between DTC, the U.S. exporter, and the foreign parties involved and constitute authorization for the export of defined "defense articles" and "defense services." Before approving the agreement, DTC reviews the underlying commercial undertaking giving rise to the need for the agreement authorization. Exports of technical data specifically authorized under an agreement may be subsequently made without separate license.

The following agreements are provided for under the ITAR:

- **The Technical Assistance Agreement ("TAA").** The TAA is a contract entered into with DTC, the exporter, and specified foreign recipients for the performance of defense services or disclosure of technical data. TAAs are often used for research and development purposes, but not for manufacturing "defense articles."
- **The Manufacturing License Agreement ("MLA")**. The MLA authorizes a foreign person to manufacture or produce "defense articles" abroad on behalf of a U.S. person. Under an MLA, both technology and "defense services" can be exported, as well as defense products under specific conditions. If Significant Military Equipment ("SME") is involved, the exporter must obtain DTC approval prior to even making a proposal to a foreign person to enter into an MLA.
- **The Distribution Agreement ("DA").** The DA constitutes approval for a U.S. exporter to export "defense articles' to distribution points or warehouses outside of the U.S., eliminating the need for a separate export license for each shipment.

The ITAR prescribe various standard clauses and provisions for all TAAs, MLAs, and DAs, and DTC may also impose specific "provisos" or conditions.

4. Comprehensive Authorizations

Various comprehensive licenses are available for use under circumstances where all anticipated export needs can be articulated and described at the start of the project, making a comprehensive authorization appropriate. These authorizations are often used to facilitate procurement of "defense articles" by U.S. allies under major joint projects, or to export items in furtherance of defense agreements between the U.S. and its allies.

5. Temporary Imports of Defense Articles

Temporary imports of "defense articles" may occur where the item is imported into the United States temporarily, for repair or exhibition purposes and then returned to the country that exported it, or because it is transiting through the United States en route to a third country. Temporary imports of these items require a prior license issued by DTC. Temporary imports of unclassified "defense articles" are subject to specific licensing exemptions.

E. Empowered Officials and Certifications

Each ITAR registrant must designate a U.S. person directly employed by the registrant, and holding a position of authority within the registrant organization, to be the "Empowered Official." The Empowered Official must be legally empowered in writing by the registrant to sign license applications and other authorization requests on behalf of the registrant. The Empowered Official certifies to the correctness of, and is held accountable for, all representations made to DTC.

F. Congressional Notification

With respect to the following exports, DTC is required to notify Congress and permit Congressional review during a 30-day waiting period:

- Contracts of at least $14 million for export or third country transfer of "Major Defense Equipment" (SME with a nonrecurring research and development cost of $50 million or more, or total production costs of at least $200 million);
- Contracts of at least $50 million for export of any defense articles or services; and
- MLAs or TAAs involving the production of SME in any non-NATO country.

If Congress issues a joint resolution disapproving the proposed transaction by the end of the 30-day period, a license will be denied. The requirement of Congressional notification applies even to ITAR-controlled exports which are not subject to licensing because of the applicability of a license exemption.

G. Political Contributions, Fees and Commissions

For sales of defense articles or services under a contract with a value of at least $500,000, the exporter must certify whether the exporter or its vendors or suppliers have directly or indirectly paid, or offered or agreed to pay, with respect to the sale transaction (i) political contributions in an amount totaling at least $5,000, or (ii) fees or commissions totaling at least $100,000. If an affirmative certification is given, the exporter must provide detailed, specified information about the payments.

H. Definitions of Key ITAR Terms

Part 120 of the ITAR contains most definitions applicable to exports of defense articles and services; other sections of the ITAR also contain relevant definitions. Following are definitions of some of the more frequently-used terms, with citations to the sections of the ITAR where they appear.

The April 16, 2013 final DTC rule revised some definitions, most notably the definitions of System (§121.8(g)) and Technical Data (§ 120.10), and added a new definition for Subject to the Export Administration Regulations (§120.42).

1. Accessories and Attachments (§121.8(c))

Accessories and attachments are associated equipment for any component, end-item or system, and which are not necessary for their operation, but which enhance their usefulness or effectiveness (e.g., military riflescopes, special paints, etc.).

2. Broker (§129.2) [20]

Broker means any person who acts as an agent for others in negotiating or arranging contracts, purchases, sales, or transfers of defense articles or defense services in return for a fee, commission, or other consideration.

3. Brokering Activities (§129.2) [21]

Brokering Activities means acting as a broker (as defined above), and includes the financing, transportation, freight forwarding, or taking of a defense article or defense service, irrespective of its origin (including foreign defense articles or services).

4. Build to Print (§124.13)

Means producing an end-item (e.g., system, subsystem, component, or part) from technical drawings and specifications (which contain no process or know-how information) without the need for additional technical assistance. Build-to-Print does not include any information which discloses design methodology, engineering analysis, detailed process information or manufacturing know-how.

5. Component (§121.8(b))

A component is an item that is useful only when used in conjunction with an end-item. A major component includes any assembled element, which forms a portion of an end-item without which the end-item is inoperable (e.g., airframes, tail sections, transmissions, tank treads, hulls, etc.). A minor component includes any assembled element of a major component.

6. Defense Article (§120.6)

Any item or technical data designated in the USML (ITAR § 121.1), including technical data recorded or stored in any physical form, models, mock-ups or other items that reveal technical data directly relating to items designated in the USML. It does not include basic marketing information on function or purpose or general system descriptions.

It should be emphasized that ITAR § 120.3 vests DTC with considerable discretion in determining which items and technical data are considered to be defense articles. Therefore, caution should be exercised in relying on self-assessments that an item or technical data do not qualify as defense articles, because such self-assessments can be, and often are, second-guessed by DTC.

7. Defense Service (§120.9)[22]

"Defense Service" means:

- The furnishing of assistance (including training) to foreign persons, whether in the United States or abroad in the design, development, engineering, manufacture, production, assembly, testing, repair, maintenance, modification, operation, demilitarization, destruction, processing, or use of defense articles;
- The furnishing to foreign persons of any technical data controlled under the ITAR, whether 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 by correspondence courses, technical, educational, or information publications and media of all kinds, training aid, orientation training exercise, and military advice.

8. Empowered Official (§ 120.25)

"Empowered Official" means a U.S. person who:

- Is directly employed by the applicant or a subsidiary in a position having authority for policy or management within the applicant organization; and

- Is legally empowered in writing by the applicant to sign license applications or other requests for approval on behalf of the applicant; and
- Understands the provisions and requirements of the various export control laws and regulations, and the criminal liability, civil liability, and administrative penalties for violating these laws and regulations; and
- Has the independent authority to: (i) Inquire into any aspect of a proposed export or temporary import; (ii) verify the legality of the transaction and the accuracy of the information to be submitted; and (iii) refuse to sign any license application or other request for approval without prejudice or other adverse recourse.

9. End-Item (§121.8(a))

An end-item is an assembled article ready for its intended use. Only ammunition, fuel, or another energy source is required to place it in an operating state.

10. Export (§120.17)

"Export" means:

- Sending or taking a defense article out of the United States in any manner, except by mere travel outside of the U.S by a person whose personal knowledge includes technical data;
- Transferring registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether in the United States or abroad;
- Disclosing (including oral or visual disclosure) or transferring in the United States any defense article to an embassy, any agency or subdivision of a foreign government (e.g., diplomatic missions);
- Disclosing (including oral or visual disclosure) or transferring technical data to a foreign person, whether in the United States or abroad; and
- Performing a defense service on behalf of, or for the benefit of a foreign person, whether in the United States or abroad.

A launch vehicle or payload is not, by reason of the launching of such vehicle, an export, although ITAR may apply to a sale, transfer, or proposal to sell or transfer the vehicle.

11. Firmware (§121.8(e))

Firmware and any related unique support tools (such as computers, linkers, editors, test case generators, diagnostic checkers, library of functions and system test diagnostics) specifically

designed for equipment or systems covered under any category of the U.S. Munitions List are considered as part of the end-item or component. Firmware includes but is not limited to circuits into which software has been programmed.

12. Foreign Person (§120.16)

Foreign person means any natural person who is not a lawful permanent resident as defined by 8 U.S.C § 1101(a)(20) or who is not a protected individual as defined by 8 U.S.C. § 1324b(a)(3). It also means any foreign corporation, business association, partnership, or any other entity or group that is not incorporated or organized to do business in the United States, as well as international organizations, foreign governments, and any agency or subdivision of foreign governments (e.g., diplomatic missions).

13. Major Defense Equipment (§120.8)

Major defense equipment means any item of significant military equipment (as defined in 22 C.F.R. § 120.7) on the USML having a nonrecurring research and development cost of more than $50,000,000 or a total production cost of more than $200,000,000.

14. Manufacturing License Agreement (§120.21)

An agreement (e.g., contract) whereby a U.S. person grants a foreign person an authorization to manufacture defense articles abroad and which involves or contemplates:

- The export of technical data (as defined in 22 C.F.R. § 120.10) or defense articles or the performance of a defense service; or
- The use by the foreign person of technical data or defense articles previously exported by the U.S. person.

15. Part (§121.8(d))

A part is any single unassembled element of a major or a minor component, accessory, or attachment which is not normally subject to disassembly without the destruction or the impairment of design use (e.g., rivets, wire, bolts, etc.).

16. Person (§120.14)

Person means a natural person as well as a corporation, business association, partnership, society, trust, or any other entity, organization or group, including governmental entities. If a provision in the ITAR does not refer exclusively to a "foreign person" or a "U.S. person" then it refers to both.

17. Public Domain (Including Fundamental Research) (§120.11)

Information which is published and generally accessible or available to the public:

- Through sales at newsstands and bookstores;
- Through subscriptions which are available without restriction to any individual who desires to obtain or purchase the published information;
- Through second-class mailing privileges granted by the U.S. Government;
- At libraries open to the public or from which the public can obtain documents;
- Through patents available at any patent office;
- Through unlimited distribution at a conference, meeting, seminar, trade show, or exhibition generally accessible to the public in the United States;
- Through public release (i.e., unlimited distribution) in any form (e.g., not necessarily in published form) after approval by the cognizant U.S. Government department or agency; or
- Through fundamental research in science and engineering at accredited institutions of higher learning in the United States where the resulting information is ordinarily published and shared broadly within the scientific community.

"Fundamental research" means basic and applied research in science and engineering where the resulting information is ordinarily published and shared broadly within the scientific community, as distinguished from research the results of which are restricted for proprietary reasons or specific U.S. Government access and dissemination controls. University research will not be considered fundamental research if (i) the university or its researchers accept other restrictions on publication of scientific and technical information resulting from the project or activity, or (ii) the research is funded by the U.S. Government and specific access and dissemination controls protecting information resulting from the research are applicable.

18. Re-export and Retransfer (§120.19)

Re-export and retransfer means the transfer of defense articles or defense services to an end use, end user, or destination not previously authorized.

19. Significant Military Equipment (§120.7)

"Significant Military Equipment" means articles for which special export controls are warranted because of their capacity for substantial military utility or capability, and includes:

- Items on the USML which are preceded by an asterisk; and
- All classified articles enumerated on the USML.

20. Software (§121.8(f))

Software includes, but is not limited to, the system functional design, logic flow, algorithms, application programs, operating systems and support software for design, implementation, test operation, diagnosis, and repair.

21. System (§121.8(g))

A system is a combination of end-items, parts, components, accessories, attachments, firmware, or software that operate together to perform a specialized military function.

22. Subject to the Export Administration Regulations (§120.42)

Items "subject to the EAR" are those items listed on the CCL in part 774 of the EAR and all other items that meet the definition of that term in accordance with § 734.3 of the EAR.

23. Technical Assistance Agreement (§120.22)

An agreement (*e.g.*, contract) for the performance of a defense services(s) or the disclosure of technical data, as opposed to an agreement granting a right or license to manufacture defense articles. Assembly of defense articles is included under this section, provided production rights or manufacturing know-how are not conveyed. Should such rights be transferred, approval of a Manufacturing License Agreement under the terms of § 120.21 is required.

24. Technical Data (§120.10)

"Technical Data" means:

- Information, other than software, as defined in § 120.10(a)(4), which is required for the design, development, production, manufacture, assembly, operation, repair, testing, maintenance, or modification of defense articles. This includes information in the form of blueprints, drawings, photographs, plans, instructions, or documentation;
- Classified information relating to defense articles and defense services on the U.S. Munitions List and 600-Series items controlled by the Commerce Control List;
- Information covered by an invention secrecy order; and
- Software as defined in § 121.8(f) directly related to defense articles.

This definition does not include information concerning general scientific, mathematical, or engineering principles commonly taught in schools, colleges, and universities or information in the public domain (*see* § 120.11). Also not included in this definition are basic marketing information on function or purpose, and general system descriptions of defense articles.

25. U.S. Person (§120.15)

U.S. person means a person (as defined in § 120.14) who is a lawful permanent resident (as defined by 8 U.S.C. § 1101(a)(20)) or who is a protected individual (as defined by 8 U.S.C. § 1324b(a)(3)). It also means any corporation, business association, partnership, society, trust, or any other entity, organization, or group that is incorporated to do business in the United States. It also includes any governmental (federal, state, or local) entity. It does not include any foreign person (as defined in § 120.16).

VII. The OFAC Regulations

Whether or not a license is otherwise required under the EAR or the ITAR, exports—and indeed perhaps any transaction or dealing at all—may be prohibited because the destination, end-use, or end-user is subject to one of several U.S. sanctions programs. The United States maintains several lists of parties, countries, and activities with which U.S. persons are prohibited or restricted from being involved. The sanctions are imposed *in addition to* U.S. export controls under other regulatory regimes, such as the EAR and the ITAR, and override any authorizations otherwise available under these export regimes.

OFAC is the primary enforcement agency for U.S. sanctions programs. OFAC acts under Presidential national emergency powers, as well as authority granted by specific legislation, to impose controls on transactions and assets within U.S. jurisdiction.

OFAC regulations apply to all persons subject to U.S. jurisdiction. This includes U.S. citizens and permanent resident aliens wherever they are located; any individual or entity located in the U.S.; corporations organized under U.S. laws, including foreign branches; and entities owned or controlled by any of the above, the most important being foreign-organized subsidiaries of U.S. corporations.

A. Proscribed Countries

OFAC administers several embargoes maintained by the U.S. against other countries. Exports to these countries and/or all other business dealings may be prohibited absent OFAC authorization. Currently, U.S. law prohibits doing most business with Cuba, Iran, and certain areas of Sudan. More narrowly targeted sanctions are maintained against other designated countries such as North Korea, Syria, and Burma. Sanctions programs are subject to periodic revisions, and companies must keep abreast of current lists of sanctioned countries and the extent to which they are sanctioned.

Of particular note, on August 10, 2012, the President signed the Iran Threat Reduction Act ("ITRA") into law. The ITRA expands the reach of certain OFAC regulations pertaining to Iran by requiring the President to act when non-US firms directly or indirectly transact business with Iran. ITRA imposes liability on a US entity or person for the activities of a non-US entity that it owns or controls, if the non-U.S. entity knowingly transacts business with the Iranian Government. The ITRA also expands the reach of OFAC civil penalties by allowing sanctions to be imposed against both the business or corporation and the officers/principals in their personal capacity.

B. "Nationals" and "Specially Designated Nationals"

Persons subject to U.S. jurisdiction are also prohibited from dealing with nationals of sanctioned countries to the same extent the country is sanctioned. The term "nationals" includes both persons and entities incorporated in those countries.

In addition, OFAC publishes a list of entities or individuals owned or controlled by, or acting for or on behalf of, targeted countries. These are known as "specially designated nationals," and the list is called the Specially Designated Nationals List ("SDNL") and is appended to the OFAC regulations. In addition, the SDNL includes other individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. The SDNL is frequently updated. In general, no one subject to U.S. jurisdiction may participate in ***any*** activity with ***anyone*** on the SDNL.

C. What Activity/Conduct Is Prohibited

No two of the sanctions programs are alike; each imposes different types and degrees of sanctions. However, prohibited transactions under the sanctions programs can include:

- Any payment or transfer to any such designated foreign country or national;
- Any export or withdrawal from the United States to a designated foreign country;
- Importation of and dealings in certain merchandise;
- Transactions with respect to securities registered or inscribed in the name of a designated national; and
- Any transfer of credit or payment of an obligation involving such designated foreign country, person, or entity.

The regulations also allow for "blocking" or "freezing" assets of designated nationals. The term "blocking" or "freezing" is used to describe a form of controlling assets under U.S. jurisdiction. While title to blocked property remains with the designated country or national, exercise of the powers and privileges associated with ownership is prohibited without OFAC authorization. Blocking imposes an across-the-board prohibition against transfers or transactions of any kind with regard to any property. Anyone subject to the regulations may not be involved with account

payments, transfers, withdrawals, or other dealings with those accounts unless authorized by OFAC.

OFAC regulations also define the type of property that is subject to control. Property is broadly defined to include: Money, checks, drafts, debts, indebtedness, obligations, notes, warehouse receipts, bills of sale, negotiable instruments, contracts, goods, wares, merchandise, ships, goods on ships, and any other property, real, personal, or mixed, tangible or intangible, or interest or interests therein, present, future, or contingent.

D. Permissible Letters of Intent and Discussions

In general, persons subject to U.S. jurisdiction are permitted to engage in business discussions and even enter into letters of intent (so long as they are non-binding) in all countries targeted with sanctions. Binding contracts, however, are generally prohibited without a license or an available license exception.

E. Licensing Procedure under OFAC Regulations

U.S. persons must obtain licenses before they may engage in activities prohibited by the OFAC regulations. In limited cases, OFAC will provide general and special licenses to permit a U.S. person to engage in otherwise prohibited activities. "General licenses" are similar to the license exceptions of the EAR. In contrast, specific licenses, which are issued by OFAC on a case-by-case basis, authorize particular individuals or entities to participate in an activity that would otherwise be prohibited by the embargo or sanctions programs. Specific licenses are granted sparingly and, if granted, are valid only for the *specific activity* proposed on the application. Generally, there are no particular forms which must be used to request licenses from OFAC. License requests must include a detailed description of the proposed transaction and the names and addresses of any individuals or companies involved.

F. Definitions of Key Terms under OFAC Regulations

Part 500, Subpart C, contains general definitions under the OFAC regulations. (*See* §§ 500.301 – 500.302). General definitions of relevance are set forth below. However, each embargo regime may contain unique definitions in addition to the general definitions.

1. Foreign Country

Foreign country includes the state and government of any such territory, as well as any political subdivision, agency, instrumentality, or other entity having or claiming control, authority, jurisdiction, or sovereignty over the territory, or any person acting or purporting to act directly or indirectly for the benefit or on behalf of the foregoing.

2. National

The term "national" includes a subject or citizen of a country or any person domiciled in or a permanent resident of a country (except persons resident or domiciled there in the service of the U.S.); any partnership, association, corporation, or other organization organized under the laws of or having its principal place of business in a country, or which is owned or controlled directly or indirectly by the government of a country; and any person acting or purporting to act directly or indirectly for the benefit or on behalf of a national of a country.

3. Nationals of More Than One Foreign Country

Any person who is a national of more than one foreign country shall be deemed to be a national of each of such foreign countries.

4. Specially Designated National

"Specially Designated National" means a person determined by the Secretary of Treasury to be a specially designated national, any person acting for or on behalf of a designated foreign country, and any partnership, association, corporation, or other organization owned or controlled directly or indirectly by the Government of a designated foreign country or of a designated foreign national.

5. Person

A person means an individual, partnership, association, corporation, or other organization.

6. Transactions

Transactions means any payment or transfer to any designated foreign country or national, the export or withdrawal from the United States to such designated foreign country, and any transfer of credit or payment of an obligation in the currency of such designated foreign country.

7. Transfer

Transfer means any actual or purported act or transaction, whether or not in writing and whether or not performed within the U.S., which has the purpose, intent or effect of creating, surrendering, releasing, transferring, or altering rights or possession of property.

8. Property

Property means any real, personal, tangible or intangible property, or interest or interests therein, whether present, future, or contingent.

9. Interest

The term "interest" when used with respect to property means an interest of any nature whatsoever, direct or indirect.

10. Person Subject to the Jurisdiction of the U.S.

A person subject to the jurisdiction of the U.S. includes any individual, wherever located, who is a citizen or resident of the U.S.; any person within the U.S.; any corporation organized under the laws of the U.S. or of any state, territory, possession, or district of the U.S.; and any corporation, partnership, or association, wherever organized or doing business, that is owned or controlled by the aforementioned persons.

11. Person within the U.S.

A person within the U.S. includes any person, wherever located, who is a resident of the U.S.; any person actually within the U.S.; any corporation organized under the laws of the U.S. or of any state, territory, possession, or district of the U.S.; and any partnership, association, corporation, or other organization, wherever organized or doing business, which is owned or controlled by any of the aforementioned persons.

VIII. Enforcement of U.S. Export Control Laws

There have been an increasing number of enforcement actions under U.S. export and sanctions laws, particularly since the September 11, 2001 terrorist attacks. Violations of these laws can result in substantial civil or criminal penalties. In addition, violations can cause the suspension or revocation of any license or other approval, detention and seizure of suspect shipments, loss of security clearances, and loss of export privileges. Recent cases indicate that the conviction rate under these laws remains high, and that judges comply strictly with the Federal Sentencing Guidelines in imposing sentences against individuals and entities convicted of violations.

A. Statutory Penalties

Violations of the export and sanctions laws may result in criminal or civil prosecutions, the imposition of fines, and such administrative penalties as forfeiture of property (or any interest therein) or denial of export privileges. If willful violation of these laws is demonstrated, violators may be subject to both criminal fines and administrative penalties. However, it is important to emphasize that there is no intent requirement for imposing administrative violations.

Under both the EAR and the OFAC regulations, penalties for civil violations can reach as high as $250,000 or twice the value of the transaction, whichever is greater, for each violation. For civil violations of the ITAR, penalties can be as high as $500,000.

For criminal violations of the EAR and ITAR, violators may be fined up to $1,000,000 and/or face up to twenty (20) years of imprisonment for each violation. For violations of the OFAC regulations, criminal penalties can include fines ranging from $50,000 to $10,000,000 and imprisonment ranging from ten (10) to thirty (30) years for willful violations.

B. What Constitutes a Violation

The penalties described above can be imposed for *each* violation of the applicable laws. Seldom will a transaction prohibited under these laws give rise to only one violation. There are numerous ways in which the laws can be violated, including by:

- Exporting or attempting to export or re-export, or causing to be exported or re-exported, any item for which a license or written approval is required without first obtaining the required license or written approval;
- Conspiring to export or re-export, or cause to be exported or re-exported, any item for which a license or written approval is required without first obtaining the required license or written approval;
- Violating any of the terms or conditions of licenses or approvals;
- Willfully causing, or aiding, abetting, counseling, demanding, inducing, procuring, or permitting the commission of any act prohibited by the applicable export/sanctions law or any regulation, license, or approval issued thereunder;
- Using false or misleading statements or omitting a material fact on any export control document;
- Willfully evading compliance with the applicable export/sanctions law;
- Possessing goods or technology with the intent to violate export restrictions or with the knowledge or reason to believe the goods will be exported illegally;
- Failing to report a violation; and
- Failing to comply with recordkeeping requirements.

C. Contractual Duties of Government Contractors

In 2010, the Department of Defense ("DoD") amended the Department of Defense Federal Acquisition Regulation Supplement ("DFARS") to require that all solicitations and contracts contain a clause articulating the contractor's export control compliance responsibilities. In addition to the statutory and regulatory burdens, the clause creates a contractual obligation to comply with export controls.[23] The clause is required to be included even if exports are not anticipated under the contract. Importantly, the clause must be included in all subcontracts entered into pursuant to

the prime contract award. The DFARS clause is similar to the contractual obligation created by the Federal Acquisition Regulations requiring contractors and subcontractors to comply with the Office of Foreign Assets Control ("OFAC") regulations governing economic sanctions.[24]

D. Role of Voluntary Disclosures

The Departments of Commerce, State and Treasury strongly encourage the self-disclosure of information to them pursuant to their respective enforcement regime by persons, firms, or any organization that believes they may have violated any provision of the applicable laws or regulations. Voluntary self-disclosure may be considered a mitigating factor in determining the penalties, if any, that can be imposed for violations. Failure to report such violation(s) may result in circumstances detrimental to U.S. national security and foreign policy interests. To be effective as a basis for mitigation, disclosures must occur before the agency to whom disclosure is made (or any other agency of the U.S. Government) has learned the same, or substantially similar information. A voluntary disclosure, however, does not absolve a company from wrongdoing.

The agencies retain the sole discretion to consider whether a voluntary disclosure, in the context of other relevant information in a particular case, should be a mitigating factor in determining whether and to what extent penalties will be imposed. Among the factors or circumstances the agency will consider when evaluating the effect of a voluntary disclosure are:

- Whether the transaction would have been authorized, and under what conditions, had a proper license request been made;
- Why the violation occurred;
- The degree of cooperation with the ensuing investigation;
- Whether the person has instituted or improved an internal compliance program to reduce the likelihood of future violations;
- Whether the person making the disclosure did so with the full knowledge and authorization of the person's senior management (if not, the agency will not view the disclosure as "voluntary");
- Whether the violation was intentional or inadvertent;
- The degree to which the person responsible for the violation was familiar with the applicable laws and regulations;
- Whether the person responsible for the violations was the subject of prior administrative or criminal action; and
- Whether the violations are systemic.

Recently, BIS revised the EAR's Voluntary Self-Disclosures ("VSD") program to specify a 180-day deadline for submitting a final and comprehensive narrative account of the violation. The regulations require the final narrative to be filed after submission of the initial VSD filing. The 180-day filing deadline applies to all initial VSDs received by BIS on or after September 9, 2013. The 180-day deadline to complete the VSD is consistent with the disclosure rules of other enforcement agencies, including DTC and OFAC both of which impose deadlines for submission of the final self-disclosure narrative. BIS's Office of Export Enforcement is authorized to extend the 180-day deadline if the disclosing party can demonstrate that more time is "reasonably necessary" to complete the final narrative account.

E. Enforcement of Export and Sanctions Laws in Other Countries

Although many traditional United States allies, like the European Union members, have long had well- established export control regimes, other countries have recently started to adopt or expand their export controls. A small sampling of countries that have passed such laws during the past several years include Mongolia, Malaysia[25], Thailand, Philippines, and the United Arab Emirates. As a result, exporters may be required to obtain licenses in any country controlling an item at any point in the transaction, regardless of whether an export or reexport license is required from the country where the exported item originated. Complicating the resulting compliance challenge is the fact that actual enforcement of export control regimes varies from country to country, making it imperative that companies doing business overseas be aware of differing enforcement climates in the countries within which they do business. Moreover, there is an unfortunate lack of coordination among countries with respect to enforcement of export laws, exposing companies to the risk of duplicative and inconsistent enforcement activity.

Like export controls, other countries have also enacted or expanded laws imposing sanctions similar to those imposed by the United States, and are increasing enforcement efforts under those laws. "Anti-money laundering" ("AML") or "know your customer" ("KYC") laws have been expanded in several countries including Brazil[26] and Vietnam.[27]

IX. Developing an Internal Compliance Program

Because of the serious consequences of noncompliance with export and sanctions laws, developing a credible internal compliance program is highly advisable. The benefits of such a program are many and include:

- Mitigation of penalties imposed for violations;
- Meeting the expectations of government enforcement officials who conduct audits or investigations;
- Preventing violations in the first place;
- Detecting and managing violations that do occur; and

- Complying with those regulations that mandate an internal compliance program.

The commitment to internal compliance must be real and credible. The consequences of having a poorly developed or maintained compliance program may be worse than having no compliance program at all. Moreover, each business must assess the elements of a robust compliance program that are appropriate for, and workable within, its unique internal and market dynamics.

Recognizing the ways in which every-day business can fall within the scope of the various export and sanctions regimes, and how properly to respond, is vitally important for any business that engages in cross-border transactions or dealings with foreign nationals. Without that self-awareness, compliance with legal and regulatory obligations can never happen, and a company is at risk of exposing it and its employees to substantial civil or criminal penalties. That self-awareness, and commitment to necessary follow-up, is also at the root of every credible internal compliance program.

A. An Internal Compliance Program Must Be Credible

Enforcement agencies will typically mitigate penalties if a violator has in place a credible internal compliance program designed to prevent violations and to detect violations when they do occur. But, mitigation depends upon convincing the enforcement agencies that a *credible* internal compliance program is in place and is being maintained. A credible internal compliance program must meet the following minimum requirements under regulatory mandates and Federal Sentencing Guidelines:

- Policy statement from senior corporate management demonstrating strong, unequivocal commitment to compliance with U.S. laws regulating international trade and business;
- List of corporate officials responsible for compliance efforts within the company;
- Written policies and procedures governing international trade and business;
- Clear and concise summary of the requirements of applicable U.S. laws and regulations, including the Foreign Corrupt Practices Act, the Export Administration Act, the Export Administration Regulations, the Anti-boycott Regulations, the Arms Export Controls Act, the International Traffic in Arms Regulations, the Trading with the Enemy Act, and the Foreign Assets Control Regulations;
- Development of order processing flow charts (computerized and/or manual);
- Development of recordkeeping processes (computerized and/or manual);
- Development of consistent and coherent system-wide training programs and schedules;
- Development of internal review and audit processes;
- Establishment of notification procedures in case of violations;

- Statement and implementation of specifically enumerated legal penalties and company disciplinary actions applicable to employees who violate laws and regulations; and

- Checklists for required screening against the Denied Parties List, the Specially Designated Nationals List, the Enhanced Proliferation Control Initiative Restrictions, the Missile Control Lists, the Nuclear Lists, the Supplement 4 Denied Entities List, and other applicable screens (computerized and/or manual).

B. Assessing the Company's Unique Compliance Obligations

Whether and to what extent a company's activities implicate export and sanctions laws depends entirely on the nature of those activities. The development of a credible internal compliance program requires initial self-assessments by a company with respect to the nature and scope of its international activities, its current compliance practices, and its history of compliance.

The following are suggested steps and self-assessment questions to initiate the process of understanding a company's internal compliance needs.

- Understand the company's international activities by assessing:

    - Which company facilities are engaged in international business activities, i.e., export, import, leasing, investment, contracting;
    - What are the geographic areas of future international expansion;
    - What company products and services are sold abroad;
    - What are the current and future markets for company products and services; and
    - Who are the company's current or likely future foreign suppliers.

- Assess the organization of the company's international activities by determining:

    - Whether the company's activities are centralized or decentralized;
    - Who has the international sales or marketing responsibilities;
    - Who are the other international "players": internal purchasing, chief financial officer, contract administration, order processing, shipping and transportation, scheduling/administration, field/service activities, operations, business development/marketing, legal;
    - How international contracts are reviewed or approved;
    - Who are the company's foreign representatives, agents, and partners;
    - Does the company use standard form contracts for international transactions; and;
    - What records are kept of international shipments.

- Examine the company's current compliance and history of compliance and ascertain the:
    - Track record of the company;
    - Track records of company employees who are international "players";
    - Attitudes of company management toward compliance;
    - Resources available for compliance; and
    - Company's experience with ICPs or business ethic programs.

- Assess the compliance strategy that best suits the company's business by considering:
    - To which countries/customers the company should market;
    - From what countries/suppliers the company should purchase;
    - For exporting activities, what type of export licensing strategy is available and preferable, e.g., comprehensive licenses under the EAR, technical assistance or manufacturing agreements under ITAR;
    - Whether there are ways to structure the company's international activities to the best advantage of the regulatory requirements; and
    - Whether there are ways to draft company contracts to better meet regulatory requirements.

C. Molding the Compliance Program to the Company's Needs

Each company's compliance structure must truly be its own, from top-level policy pronouncements to implementing procedures. Based on its assessment of the nature of its global business activities and the specific ways in which its activities confront export and sanctions control obligations, a company will need to:

- Articulate the general rules of conduct, ethical or legal, to be adopted as policies by the company;
- Specify the detailed procedures to implement these policies;
- Designate a chief compliance officer with overall responsibility for compliance;
- Designate appropriate subordinate officers with compliance responsibility;
- Delineate the role of the company's in-house lawyers and assume continued protection of the attorney-client privilege;
- Delineate the oversight role of the Board of Directors;

- Specify control requirements, e.g., two signature requirements for disbursement of significant funds or designated person for approval of certain transactions;
- Determine a system for reporting violations, e.g., "hotline," suggestions box, whistleblower protection;
- Articulate disciplinary measures and standard for violators;
- Develop standard contracts or contract checklist containing appropriate provisions that are consistent with export/sanctions requirements; and
- Commit to the use of "self-policing" tools, such as audits, investigations, and due diligence reviews.

D. Components of an Effective Compliance Program

There are several essential "building blocks" of an internal compliance program.

1. Buy-in from Company Leadership

An enforcement agency will not view an internal compliance program as credible that does not have the solid and visible endorsement of senior management. Thus, a credible internal compliance program must:

- Outline and emphasize senior management's commitment to compliance with all applicable laws and regulations;
- Emphasize the significance of laws and regulations governing the company's international business;
- Be communicated to all levels within the company;
- Come from senior company management directly; and
- Notify company employees of their obligations and the disciplinary consequences of failure to satisfy those obligations.

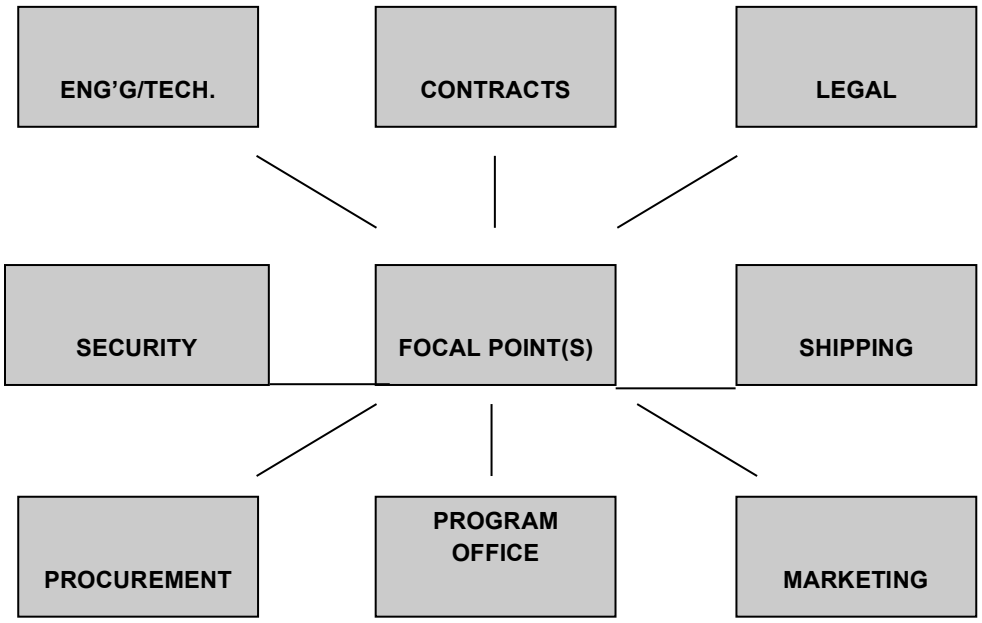
2. A Workable Structure and Designation of Focal Points

A credible internal compliance program has a workable structure and designated persons charged with the responsibility of, and with accountability for, overseeing compliance. There are several attributes of a workable compliance oversight function, as follows:

- Company must designate specific, readily identifiable individuals as *focal points* responsible for company compliance;
- Sales personnel should not be designated as *focal points*, i.e., the export manager and the director of sales should be different people;
- The *focal points* must be knowledgeable and well-trained in all facets of applicable laws and regulations;
- The *focal points* should be identified by position, office, and telephone numbers; and
- The identification of *focal points* must be communicated to all levels within the company.

Moreover, the organization of the focal point's responsibilities must recognize and address lines of responsible oversight with respect to all functional units within the business who are involved in cross-border transactions or encounters with foreign nationals.

The following schematic depicts some of the business areas of a company that may confront or be involved in the resolution of export/sanctions compliance issues. The schematic is intended to underscore the central role that the export/sanctions focal point(s) must play.



Each of the business areas represented in the schematic should have defined tasks with respect to a company's export/sanctions program that derive from their areas functions. The following is offered as an illustration of responsibilities associated with the business areas depicted above.

- Focal Point(s)
    - Business segment/site focal points for export and sanctions compliance.

- Determine need for license/USG authorizations.
- Coordinate with Contracts Administrators, Program Managers, and Engineering.
- Coordinate preparation of applications.
- Review and submit license/authorization applications.
- Coordinate follow-up information/communications.
- Receive and transmit approvals to business segment/site focal points.
- Interpret regulatory requirements; consult with Legal.
- Maintain records of applications/approvals.
- Coordinate required reporting.
- Coordinate with Legal for employee training programs.

■ Contracts Administration

- Prepare applications for license; coordinate with Program and Focal Point.
- Retain original licenses/transmit originals to Shipping; maintain copies.
- Prepare/submit required reports.
- Prepare technical control plans for foreign national visit/hire.
- Supply Shipping with required documentation.
- Advise Focal Point on activity and status of active licenses.
- Administer active licenses; responsible for controlling, documenting, recordkeeping, and reporting to Focal Point.

■ Program Office

- Provide overall guidance to Focal Point and Contracts on all programs involving exports.
- Identify export related program requirements, including offshore procurement.
- Determine technical baseline documents to be disclosed to foreign nationals.
- Submit requests for licenses to Contracts; provide supporting documentation.
- Monitor program activities against scope of licenses.
- Coordinate with Focal Point data required for Part 130 Certification.

- Marketing

    - Submit all international pre-sale, sales promotional, and business development materials to Focal Point for approval.
    - Coordinate with Focal Point obtaining required licenses.
    - Retain licenses and monitor activities against scope of authorization.

- Engineering

    - Designate business segment/site technical Focal Point to assist other functions.
    - When requested, assess whether technical data may be subject to export.
    - Forward to Focal Point requests for non-contract licenses related to conferences, technical papers, etc.

- Security

    - Provide security classification guidance and guidance on protection of technical data.
    - Provide in-plant foreign visitor control; maintain records.
    - Provide employee foreign travel control.
    - Coordinate with Human Resources on hiring of foreign nationals.
    - Coordinate with Focal Point on development and administration of technology control plan.
    - Coordinate with Shipping on transportation plans for technical data.
    - Investigate with Legal reports of possible noncompliance.

- Shipping

    - Advise on proper U.S. Customs procedures/requirements.
    - Determine mode of shipment and select appropriate carrier, forwarder, or broker.
    - Ensure shipments/documentation comply with applicable regulations.
    - Provide Focal Point with contract information and status of licenses.
    - Develop approved list of carriers, forwarders, and brokers.
    - Take corrective action to prohibit exports suspected to be in violation of law.

- Legal

    - Provide required legal advice.

- Conduct reviews and investigations in coordination with other functional organizations.

- Procurement
  - Identify foreign supplier needs.
  - Act as sole interface with foreign suppliers.
  - No responsibility for coordinating licenses or agreements.
  - Provide to Contracts necessary documentation.
  - Provide international purchase orders and necessary export approval references to Shipping.

3. Education and Training

A program of education and training employees regarding export/sanctions compliance requirements is essential to meeting the standards of an internal compliance program recognized as reasonably designed to prevent and detect violations. Therefore, provision in the internal compliance program must be made for employee education and training which:

- Ensures all employees' familiarity with compliance requirements;
- Provides for more detailed education/training for employees in international functions and "key" management positions; and
- Ensures that foreign consignees, agents, distributors, and co-venturers are familiar with and support U.S. export/sanctions rules.

Enforcement agencies will look to various characteristics of the training program when assessing the credibility of an internal compliance program. Training must be:

- Continuous;
- Current;
- Targeted to employees based upon their responsibilities;
- Regularly scheduled; and
- Conducted by clearly designated training individual(s).

4. Screening

Whether controlled by the Departments of Commerce, State or Treasury, a transaction may be prohibited because of the destination, end-use, or end-user. The U.S. Government maintains a series of lists and publishes notices of parties, countries, and activities for which exports are strictly prohibited, or otherwise restricted, and/or with whom U.S. persons are prohibited from conducting any business. Screening is viewed by U.S. enforcement agencies as an integral part of a credible internal compliance program in order to prevent and detect unlawful transactions. It is also necessary if the exporter hopes to provide justification and documentation for export decisions.

Accordingly, it is highly recommended that companies engaged in global activities institutionalize the screening of employees, consultants, customers, contractors, subcontractors, vendors, and other company business partners using the following lists prior to transferring technical data, technology or services, whether domestically or overseas, or conducting any other business:

- **Denied Persons List.** The denial or limitation of the privilege of exporting is one of many sanctions authorized under U.S. export laws. Parties denied export privileges by the Commerce Department are generally precluded from participating in any manner in any export-related transaction subject to the EAR. Sanctions can be imposed for engaging in export transactions with such "Denied Parties." U.S. exporters must therefore screen all parties to their export transactions (including freight forwarders, intermediate consignees, end-users, and others are not on the Table of Denial orders). A list is published by the Department of Commerce of persons that have been denied export privileges in whole or in part. *(See* Supplement No. 2 of Part 764 of the EAR). Most transactions with these denied persons, including exports to or from, re-exports, and intra-country transfers abroad, are prohibited without prior authorization from the U.S. Government.

- **Specially Designated Nationals List.** The OFAC publishes a list of entities with whom any transactions are prohibited without prior authorization from OFAC.

- **Debarred and Suspended Parties Lists.** The Department of State publishes a list of parties whose export privileges have been revoked or suspended. Exports to these parties are prohibited, except in rare circumstances, when it is in the national interest.

- **Proscribed Missile Technology Lists.** The Department of Commerce prohibits the export or re-export to any destination without a license of items subject to the EAR, if the exporter knows or has reason to know that the export is destined for specific missile projects, or will be used in the design, development, production or use of missiles in or by certain countries. The Department of State also controls certain missile-related items that are concurrently found on the Commerce Control List. Prior approval may be required from both the Department of State and the Department of Commerce prior to the export of these items. The EAR contains a list of missile-related facilities and technologies controlled for these purposes.

- **Proscribed Chemical and Biological Weapons List.** The Department of Commerce maintains a list of chemical and biological weapons ("CBW"), end-uses, and end-users,

for which the export of any item subject to the EAR requires a license, including items for which no license is required. Exports for the designated end-uses and end-users may not be conducted without prior authorization from the Department of Commerce.

- **Proscribed Destination Restrictions/Entities List.** Exports to destinations or entities under sanctions are strictly controlled. The Departments of Commerce and State publish lists of destinations and entities sanctioned pursuant to U.S. law.

- **Embargoed Countries.** OFAC administers embargoes that the United States maintains against other countries. Exports to these countries and/or all other business dealings are prohibited absent special authorization from OFAC. Sanctions can be imposed for engaging in export or other business transactions with these persons and entities. U.S. persons, including exporters, must therefore ensure that all parties to their transactions (including freight forwarders, intermediate consignees, end-users, and others) are not named on these lists.

Screening should be conducted by those company employees best suited to ensure that restricted transfers do not occur. Generally, screening should be performed at initial and/or interim functional control points that are likely to detect restricted transfers before an export occurs. The employee performing the screening should record that the screening was done, the date it was completed, and the employee's name.

5. Diversion Avoidance and "Red Flags"

Exporters should institutionalize "red flags" review of all orders and transactions, and provide instruction to all relevant employees regarding such review. The "red flags" checklist is published by BIS and can be found on its website. Possible indicators – or "red flags" – that an unlawful diversion might be planned by a company's customer include the following:

- The transferee is reluctant to offer information about the end-use of the items received;

- The item, technical data or services do not appear to fit the transferee's line of business; for example, a small bakery places an order for several sophisticated lasers;

- The item transferred is incompatible with the technical capability of the transferee; for example, semiconductor manufacturing equipment would be of little use in a country without an electronics industry;

- The transferee has little or no relevant background;

- The transferee is unfamiliar with the technology or technical data;

- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations;

- Performance/design requirements are incompatible with the foreign end-user's resources or environment;

- Stated end-use is incompatible with the customary or known applications for the technology or technical data; and
- The transferee responds evasively to questions regarding any of the above.

If a "red flag" exists, indicating that a transfer may violate export control policies or laws, follow-up information from the party with whom the transaction is being arranged must be requested and resolved before the transaction moves forward.

To conduct a proper "red flags" review, the exporter must:

- **Decide whether there are "red flags."** Take into account any abnormal circumstances in a transaction that indicate that the export may be destined for an inappropriate end-use, end-user, or destination. Such circumstances are referred to as "red flags." Included among examples of red flags are orders for items that are inconsistent with the needs of the purchaser, or requests for equipment configurations that are incompatible with the stated destination (e.g., 120 volts in a country with 220 volts). BIS has developed lists of such red flags that are not all-inclusive but are intended to illustrate the types of circumstances that should cause reasonable suspicion about a transaction.
- **If there are "red flags," inquire.** If there are no "red flags" in the information that comes to you, you should be able to proceed with a transaction in reliance on information you have received. That is, absent "red flags" (or an express requirement in the ITAR or EAR), there is no affirmative duty to inquire, verify, or otherwise "go behind" the customer's representations. However, when "red flags" are raised in information that comes to you, you have a duty to check out the suspicious circumstances and make appropriate inquiries.
- **Avoid self-blindness.** Do not cut off the flow of information coming to you in the normal course or put on blinders blocking the receipt of relevant information. Avoiding "bad" information does not insulate a company from liability, and could be considered an aggravating factor in an enforcement proceeding.
- **Know how to handle "red flags."** Knowledge possessed by a company's employees and representatives can be imputed to the company so as to make it liable for a violation. This makes it important for the company to establish clear policies and effective compliance procedures to ensure that such knowledge about transactions can be evaluated by responsible senior officials. Failure to do so could be regarded as a form of self-blinding.
- **Reevaluate all the information after the inquiry.** The purpose of this inquiry and reevaluation is to determine whether the "red flags" can be explained or justified. If they can, you may proceed with the transaction. If they cannot and you proceed, you run the risk of having had "knowledge" that would make your action a violation of the EAR or the ITAR.

- **Refrain from the transaction and wait.** If reasons for concern remain after this inquiry, the company should refrain from the transaction and submit all relevant information to its export control specialist for evaluation.

6. Instilling a Culture of Communication

The successful implementation of a credible internal compliance program depends upon regular and effective communications between and among designated focal points and employees involved in transactions subject to compliance requirements. Coordination of compliance efforts requires that the various functional units "talk" to one another. Communications may be necessary at variety of stages in a transaction, such as:

- **Pre-Contract Stage**. Sales/marketing must advise export compliance manager of requests for proposal or proposed sales contracts involving export transactions, and provide information on product, name of proposed customer and any related parties, location of proposed customer and place of delivery, intended use of product, contract price (estimated), proposed delivery date, any associated documentation to be delivered, whether ancillary services (training, installation, support) to be provided and if so, what, any update and enhancement obligations. The export compliance manager must advise sales/marketing on the scope of information to be provided. The export compliance manager must then determine export compliance strategy and requirements, screen proposed customer against U.S. Government lists, initiate any license applications or documentation required, review contract provisions, and communicate with sales/marketing regarding these determinations and any proposed contract revisions. Sales/marketing should allow sufficient time for the completion of this process. Sales/marketing should refrain from making any contractual commitments until the export compliance manager has completed satisfactory determinations with regard to screening and the need for a license.

- **Contract Stage.** Sales/marketing must communicate with customers and with program/order processing to make all delivery commitments subject to any necessary government approvals identified by export compliance manager review and subject to any other commitments required by export compliance manager.

- **Post-Contract Stage.** Responsible persons must refrain from shipping until the export compliance manager communicates sign-off on export control compliance, including with respect to all necessary licenses obtained and license conditions satisfied, all necessary supporting documentation obtained, destination control statement on air waybill/bill of lading and commercial invoices, Shippers Export Declaration or Shipper's Letter of Instructions prepared, other shipping documentation completed and correct, and final screening completed.

- **Re-exports.** U.S. export controls may govern the delivery of products or services to third parties by a company's subsidiaries, or delivery of products or services by employees located abroad, agents, or distributors, where the products or services originated in the U.S., incorporate U.S.-origin parts/components, or are based

substantially on U.S. technology. Delivery to a third party in the same country as the subsidiary, agent, etc. requires screening, and possibly the obtaining of documentation (such as written assurances against diversion) from that third party. Accordingly, prior to delivery, the subsidiary, agent, or employee needs to inform the export compliance manager of the identity of the third party, and needs to obtain clearance from the export compliance manager of such delivery. That clearance must include a sign-off on the third party contract terms with respect to sublicenses or re-sales of the product. Delivery to a party in a third country should be conditions upon receiving export compliance manager sign-off as with an initial export.

- **Domestic Deliveries**. With respect to any delivery of product or provision of services within the U.S., company personnel must assess whether an "export" is involved by soliciting and gathering relevant information. Questions to be asked and answers to be communicated include:

  (i) For ITAR-controlled items, is the product to be delivered or technical assistance rendered to a foreign national?;

  (ii) If a dual-use item, is the product to be delivered to a foreign national who intends to take that product abroad?;

  (iii) For both ITAR-controlled and dual-use items, is information to be disclosed to a foreign national regardless of whether s/he intends to take it abroad?;

  (iv) Is a U.S. customer actually a front organization for a foreign national who intends to take the product/information abroad?; and

  (v) Are there any other circumstances (e.g., unusual packing or marking requirements, vagueness regarding end-use, etc.) that would suggest the disposition of the product/information may be different than represented?

If information received suggests that an "export" may occur, the export compliance manager must be contacted regarding appropriate steps to be taken. No commitments or deliveries should be made prior to receipt of the export compliance manager's written authorization.

7. Internal Audits

In order to ensure that its efforts comply with U.S. export and sanctions laws and regulations, exporters should conduct regular internal audits to assess objectively and independently all aspects of its compliance efforts. An effective audit program will be:

- Designed to verify company compliance with its compliance system and all applicable laws;

- Company-wide, including all divisions, branches, units, or subsidiaries;

- Conducted by a clearly designated responsible official within the company or outside counsel; and
- Conducted annually *at a minimum.*

A proper audit involves document reviews, personnel interviews, recordkeeping analysis, and preparation of internal systems review reports. The methodology used depends upon audit objectives (i.e., procedures review, investigation, due diligence review, or acquisition). Two commonly-used types of audits are the following:

- **Policies and Procedures Audit.** This audit is a review of policies and procedures to assess whether the company effectively maintains export policies and procedures. This review is designed to identify whether applicable legal obligations are addressed throughout the company.
- **Compliance Audit.** This audit is a review of select transactions, activities, practices and procedures conducted to assess whether the company properly implements the policies and procedures of the compliance program. These reviews may be used as a precursor to investigating potential violations.

Responsibility for auditing often vests in the company counsel. Any situation requiring investigation should always be handled by company counsel.

8. Recordkeeping

Exporters are subject to multiple recordkeeping requirements related to their export activities. Both the ITAR and the EAR require that records be kept reflecting the export of defense articles, defense services, dual-use commodities, and related technologies. Exporters must maintain records in an accurate and consistent manner, readily available for inspection by the U.S. Government.

Recordkeeping responsibilities include:

- Identifying transactions for which records must be kept;
- Identifying the records that must be retained;
- Identifying persons or functions responsible for maintaining the records;
- Determining the period of time records must be kept; and
- Ensuring uniformity of substantive information and record accessibility.

The following types of transactions are subject to recordkeeping requirements:

- Exports of controlled commodities, software or technical data from the United States or by U.S. persons;
- Re-exports or transshipments of controlled products or technical data originally exported from the United States or by U.S. persons;
- Any other transaction subject to export control, whether or not the export or re-export actually occurs;
- Exports with respect to which it appears that a person in another foreign country has an interest in the transaction or that the commodity or technical data will be exported, transshipped, or diverted;
- Negotiations in connection with an export; and
- Transactions involving restrictive trade practices or boycott requirements.

All documents related to export activities must be retained, whether they involve the processes associated with obtaining licenses or the implementation of a license already approved. It is recommended that an exporter retain the following export documents and related supporting materials:

- Classification decisions;
- License applications and all supporting documents;
- Issued licenses with limitations or provisos, if any;
- International Import Certificates and applications therefore;
- Delivery Verification or similar evidence of delivery;
- Shipper's Export Declarations ("SED");
- Receipts, bills of lading and other documents related to export clearance;
- Reports of boycott requests, and all documents relating to the requests;
- Any U.S. Government document demonstrating that an export occurred;
- Purchase orders, foreign import certificates, and airway bills;
- Non-transfer and use certificates;
- Memoranda, notes, correspondence, contracts, invitations to bid, books of account, financial records, and any other writing pertaining to an export;

- Records concerning the manufacture, acquisition and disposition of defense articles and services; and
- Any other records required under *any* provisions of the EAR, the ITAR, or the OFAC regulations.

Export documents must be retained for a minimum of five (5) years, calculated from points in time specified under the EAR and ITAR. Records under the EAR must be retained for five years from the *latest* of:

- The date the export from the U.S. occurs;
- The date of any known re-export, transshipment, or diversion of such item;
- The date of any termination of the transaction; or
- The date of receipt of the boycott-related request for records of boycotts.

Records under the ITAR must be retained for five years from the *latest* of:

- Expiration of the license to which the documentation relates;
- The date the license is exhausted or used completely; or
- The date the license is suspended, revoked, or no longer valid.

The decision where to locate records must be made with reference to the obligation under both the EAR and ITAR to keep records in a manner which facilitates the ability to retrieve them for any purpose and to review them during internal or U.S. Government audits. Export records must be made available for copying and inspection *on demand* by any authorized representative of the U.S. Government (e.g., Export Enforcement Agents, Antiboycott Compliance Officers, and Customs Agents and Inspectors). Response to such a demand, however, should only be authorized by the company's legal counsel.

The following records, whether originals or back-ups, should be kept in an accessible manner, and preferably by the company official responsible for export compliance:

- The company's Department of State registration;
- Copies of license applications with supporting documentation;

- Copies of issued export authorizations, including provisos or limitations;
- Copies of U.S. Government requests for company documents;
- Copies of notices of suspension, revocation, or other similar action;
- Copies of notices of suspension or debarment against the company; and
- Any official correspondence between the company and the U.S. Government.

In the event any request for documents is received from a U.S. Government agency or representative, company legal counsel should be contacted. Employees should receive instructions, as a matter of routine training, that they must not destroy any document, even if the five (5) year retention period has expired.

In the event that enforcement authorities appear at the exporter's facility, company legal counsel should be immediately contacted. Employees should collect and retain any official U.S. Government documents, whether subpoenas or other access requests and forward them immediately to company counsel who is the only person who should provide instructions to employees on any further action. Company employees should be instructed that they may not, under any circumstances, interfere with or impede any federal law enforcement officer performing his/her official duties.

9. Notification, Reporting, and Internal Investigations

Effective implementation and administration of a company's compliance program requires ongoing and consistent cooperation between the company and its employees. An essential part of this cooperation is a mechanism for notification and reporting of violations or suspicious transactions. An available reporting structure is essential if a company hopes to:

- Consult with outside counsel or appropriate U.S. Government agency if questions arrive related to specific transactions;
- Respond to enforcement inquiries;
- Respond to antiboycott requests;
- Prepare voluntary self-disclosures to the a U.S. Government agency; and
- Reasonably verify end-uses and/or end users.

Therefore, company employees should be required to report the following events to a designated contact person *immediately*:

- Any non-routine contact by phone, letter, or in person, by a U.S. Government official or agency, including any request to review or discuss a previously issued export license or past export shipment;
- A shipment from or to the company detained or seized by U.S. Customs;
- Receipt of a subpoena or other criminal procedure notification related to U.S. export or trade laws;
- A suspected violation of company policy or law regarding exports;
- Any events triggering reporting requirements under the antiboycott and restricted trade practices regulations; and
- Any transaction requiring U.S. Government export approvals.

Notification should occur as soon as possible after any of the foregoing events. Company personnel must be instructed not to ignore or cut off the flow of information that comes to them in the normal course of business to avoid learning of violations. Knowledge possessed by company personnel can and will be imputed to the company. Therefore, a company's personnel must be encouraged to report any questionable, unauthorized, or illegal activities, whenever discovered by the employee, to the company's legal counsel for a thorough review and evaluation. Personnel should be encouraged to report sufficient information to allow the company to pursue an appropriate course of action in the event of an actual or potential violation.

Personnel should be assured that reports of possible violations can be made in confidence, without fear of retaliation or retribution against the reporting personnel. Once a violation has been reported and company legal counsel has determined that further review is necessary, counsel should immediately arrange to investigate the matter. Investigations represent targeted assessments of specific transactions, designated to determine whether violations of law or corporate policies and procedures have occurred. Initial fact-finding and legal assessments may occur at the business units.

E. Compliance Challenges: Anticipating Unexpected Exports

Every company has a unique mix of international business activities, and will differ in the manner in which it generates and implements these activities. An effective internal compliance program must anticipate export issues occurring in otherwise routine business situations that may not always be recognized by employees as sources of compliance issues.

1. Sales and Marketing Proposals

Information contained in sales and marketing proposals may contain technical data related to controlled items, in which case it would be subject to U.S. export control laws and regulations. Therefore, before submitting any proposal to a foreign person, a company's employees, wherever

located, who are engaged in sales and marketing activities must ensure that disclosures of information to prospective customers do not require prior authorization, if they are permitted at all.

The following questions help to highlight whether a company's marketing or sales activity involves information which implicates export/sanctions control rules:

- **Does information contained in marketing materials or sales proposals constitute controlled technical data?** Technical data is any information which relates to the design, development, production, manufacture, assembly, operations, repair, maintenance, or modification of an item. All data which relates to classified items, or which relates to ITAR-controlled items, should be considered controlled technical data. All technical data which is considered by a company or any of its customers to be proprietary may also be considered controlled technical data.

- **Will transfer of the sales/marketing material possibly be made to a national of a country other than the United States and, if so, of what other country?** Although U.S. export regulations typically do not differentiate the nationalities of non-U.S. persons, disclosures to nationals of some ally countries may be controlled less strictly under the ITAR.

- **Is the information contained in sales/marketing material otherwise in the public domain?** Information that is in the public domain is information which is available through sales at newsstands and book stores; through subscriptions which are available without restriction; at public libraries; under patents at any patent office; through unlimited distribution at a conference, meeting, seminar, trade show or exhibition, which is generally accessible to the public, in the U.S.; through public release after authorization from the cognizant U.S. government department or agency; or, through fundamental research from institutions of higher learning in the U.S. where the resulting information is ordinarily published and shared broadly in the scientific community, but not including such information which is withheld from publication or which is funded by the U.S. government and to which access controls apply.

If the sales/marketing information is "technical data" and will be transferred to a foreign national or destination, and it is not otherwise available in the public domain, then the transfer implicates U.S. export controls and prior authorization may be required. Sales/marketing personnel should, then, be required to consult with the applicable compliance manager before transferring technical data in the pursuit of sales opportunities which appear to implicate export control requirements.

Requirements under the ITAR can be particularly problematic. If a proposal involves SME, for example, an exporter must comply with specific ITAR requirements regarding proposals or presentations "designed to constitute a basis for a decision to purchase and enter into any Agreement." [28] Prior Approval of the Department of State is required for proposals involving hardware if:

- The proposal involves sale of SME valued at $14 million or more;

- The equipment is intended for use by armed forces of a non-NATO country or Australia, New Zealand, or Japan; and
- The sale would involve the export of any defense article or defense service (including technical data); and
- The identical SME *has not* been previously licensed for export or sold under the Foreign Military Sales Program ("FMS").

Prior *notification*, in writing, at least thirty (30) days in advance of any proposal or presentation concerning the sale of SME is required if:

- The proposal is for sale of SME valued at $14 million or more;
- The equipment is intended for use by armed forces of a non-NATO country or Australia, New Zealand, or Japan; and
- The sale would involve the export of any defense article or defense service (including technical data); and
- The identical SME *has* been previously licensed for export or sold under the Foreign Military Sales Program.

Prior ITAR authorization is also required for proposals involving technical data if:

- The proposal will result in an MLA or TAA; and
- The agreement is for the production or assembly of SME (regardless of dollar value) in any foreign country; and
- The equipment is for use by the armed forces of any foreign country; and
- The agreement would involve the export of any defense article or service, including technical data.

2. Attending Trade Shows

Worldwide trade shows with attendees from different countries may provide companies with a tremendous marketing opportunity through the display of models and the distribution of service literature. However, participation in trade shows, whether in the United States or abroad, may trigger United States export/sanctions issues. This is particularly true for manufacturers and exporters of ITAR-controlled items, whether "defense articles" or technical data related to "defense articles."

Presentations at trade shows that include the display or distribution of ITAR-controlled "technical data" (as defined in the ITAR) may require the prior approval of the U.S. government if the trade show or conference is international or is located in the United States but open to foreign nationals. In such cases, an export can occur even if no materials or products are given to trade show attendees; the mere display of certain products or information can be considered an export under U.S. law (i.e., by visual disclosure). Distribution of written material, technical conversations or discussion, and/or oral presentations may also be considered exports. Approval from the State Department is not required if technical data is already in the public domain.

ITAR registrants, therefore, may need to include in their internal compliance program procedures for obtaining the necessary U.S. government approvals when exhibiting products or information that may contain U.S.-origin technology at trade shows. With respect to trade shows outside of the United States, such procedures would need to address:

- **Display of Equipment.** For items controlled under the ITAR, a temporary export license (DSP-73) is required. If a DSP-73 is approved for the hardware, related technical data my also be exported without a license if it satisfies the exemption under 22 C.F.R. Section 125.4.

- **Release of Technical Data.** A permanent export license application (a DSP-5 for ITAR controlled items) is required for the release of "expendable" technical data. "Expendable" technical data is any written or oral technical data (e.g., operations manual, repair manuals, blueprints, engineering drawings, etc.). However, some information may be released to foreign persons without obtaining a license. Examples of such information include general marketing materials; marketing brochures describing the product and its function; performance sheets describing functional characteristics such as size, weight, power, design life, image resolution, etc.; and any information in the public domain.

Procedures would be slightly different for trade shows and conferences occurring in the United States. Controlled technical data should not be released at trade shows and conferences open to foreign nationals held in the United States without the prior approval of the cognizant U.S. government department or agency.

Examples of technical data which may require approval include:

- Operations or repair manuals;

- Discussions or a paper describing how an item operates;

- Blueprint drawings; and

- Displaying an item (if technical data would be revealed through the display).

The following considerations are relevant in assessing the need for a license to exhibit or discuss controlled technical data at a U.S.-based trade show:

- Whether the information relates to the design, development, production, manufacture, assembly operation, repair, testing, maintenance, or modification of a controlled item;
- Whether the information is or may be classified;
- Whether the information is considered confidential or proprietary by the company or one of its customers;
- Whether the information was generated or developed from work performed under a government contract;
- Whether the information will be released to foreign nationals;
- Whether the information will be presented to a target audience, and if so, are any controls on further dissemination in place;
- Whether the information will be released outside the United States; and
- Whether the information is already in the "public domain."

3. Foreign Travel

If personnel engage in international travel for a company, they must be made aware of the export compliance responsibilities they and the company have in connection with their trip. For purposes of international travel, employees must understand that:

- Items brought on the trip may be controlled, including related technical information and services;
- All proprietary and confidential information should be assumed to be controlled;
- Controlled items, services, and technical information may not be exported prior to the receipt of U.S. Government authorization;
- An export of technical information occurs when a transfer is made to a foreign person, such as during conversations with foreign persons, by giving presentations to foreign persons, or by providing access to information to a foreign person;
- Certain exemptions may apply which allow an export to occur without prior authorization, but even these exports must be fully considered and documented by the company;

- To the extent that any item, data or information is being carried overseas, or is being transferred to a foreign person during your travel, the responsible compliance manager must be consulted prior to the trip to ascertain whether an export is occurring and what exemptions or approvals may apply;

- If equipment or material is being carried for delivery overseas or for a demonstration or trade show, even if the equipment will remain in the employee's possession, an export license may be required;

- When hand-carrying hardware and/or technical data (whether under an approved license or an exemption), the employee may need a Shipper's Export Declaration ("SED") to clear Customs; and

- Although a commercial, off-the-shelf laptop may not require any prior export authorization before being taken outside of the U.S., a license may nonetheless be required before technical data stored on the laptop can be exported.

4. Posting Data on the Internet

The Internet deserves special attention because the exchange of information over this medium is often perceived as intangible and therefore not subject to export controls. Contrary to this perception, technical data posted on the Internet is controlled just as other commodities and products. The Departments of State and Commerce have determined that placing data onto the Internet is an export and must be treated as such. For this reason, all data placed onto the Internet by a company's employees must be cleared for publishing or have the necessary export approvals in place. The "publishing" of data on the Internet is treated in the same manner as the publishing of data in any other forum. The only data beyond the scope of the export controls is data that falls into one of the following criteria:

- The data is "Public Domain" as defined in § 120.11 of the ITAR, or is "Publicly Available" under Part 772 of the EAR;

- Pursuant to § 125.4(b)(13) of the ITAR, the data has been cleared for release by either the Directorate for Freedom of Information and Security Review (DFOISR) or the Cognizant U.S. Government Department or Agency; or

- Necessary export approvals to publish the data have been obtained. (This option is the most unlikely because data placed onto the Internet is available around the world and a license is unlikely to be approved for such a broad end-user base.).

5. Computer Security

The control of technical data within a company's internal computer systems is essential to effective export/sanctions control compliance. Foreign national employees should be provided with stand-alone computer systems or be fire-walled from export controlled data when on networks. Foreign nationals should not have access to the company network unless access is granted, in writing, by

the responsible compliance manager. Access to computer networks should be password controlled.

6. Cloud Computing

With the advent of modern developments in data storage technology, businesses have seen immediate advantages to switching to what is colloquially referred to as "cloud computing." Cloud computing involves a system of computer servers linked together through a network (typically the Internet), which can be located and accessed anywhere that a user has an Internet connection. Cloud computing is appealing to businesses because it offers economic advantages, such as lower up-front costs for the products and services and less infrastructure.

However, there is currently no dispositive guidance with respect to when and where "in the cloud" an export of stored data and technology may occur that would trigger licensing requirements under the export regimes. Little guidance has been forthcoming from U.S. export agencies, and the inherent qualities of cloud computing technology make it difficult to self-assess compliance issues within the current regulatory framework. The current export regimes use a location-based focus, which is ill-suited to the dynamic nature of cloud computing. Users—and even providers—may have a hard time pinpointing the exact location where data is being held because servers allocate computing resources based on spikes in activity.

U.S. export control agencies have expressed very few opinions regarding cloud computing. Two BIS advisory opinions from 2009 and 2011 ("2009 AO" and "2011 AO," respectively) provide the only substantive guidance available to cloud providers and users. The 2009 AO, addressing the types of transmissions considered exports and which party would be responsible for such exports, set forth the following major conclusions:

- Merely providing cloud technology is not an export nor is it subject to the EAR;
- A user transmitting controlled software to a foreign destination to enable cloud computing *is* subject to the EAR;
- Users exporting controlled technology to and from a cloud are subject to the EAR; and
- The cloud provider in the U.S. is *not* the exporter of any data that users place on and retrieve from their cloud (i.e., the *user* carries the compliance burden).

The 2011 AO considered how "deemed exports" fit into cloud computing. Generally, under the EAR a foreign national must have a license approved by the BIS in order to access certain restricted information or data, even if they are physically located in the United States. In its 2011 AO, BIS determined that this regulation is inapplicable to the cloud provider, reinforcing its conclusion in its 2009 AO that the burden for cloud computing will fall on the cloud user.

DTC has not released a formal opinion on the subject of cloud computing and, therefore, it is unknown whether DTC would adopt the same view as BIS, or a stricter one, with respect to cloud computing involving ITAR-controlled information.

Similarly, OFAC has not formally opined on the subject of cloud computing. However, if business transactions are prohibited with respect to certain countries, persons or entities, it seems likely that OFAC would not view the provision of cloud computing services as exempt from the prohibited transactions.

7. Foreign National Visitors

Company employees who host or participate in visits involving foreign nationals should be aware that technical data disclosed in any manner during such a visit constitutes an export that must meet applicable regulatory requirements. U.S. persons who are employees of a foreign company, or who are acting on behalf of a foreign entity, must be treated as foreign persons for purposes of export laws. Controlled data may not be provided to such individuals without an export assessment and any necessary prior approvals. If an export license is required, such a license must be obtained prior to the visit. If an export license is denied, then the visit may not occur unless only publicly available material will be discussed. To prevent the unauthorized export of technical data to foreign nationals, sufficient information must be gathered regarding the identity of foreign visitors, the nature of the visit and the kind of information to be released. A designated focal point should then assess licensing requirements.

F. Overview of an Internal Compliance Program

The following sets forth in outline format an overview of an internal compliance program designed to address export and sanctions controls issues. It is offered as an illustration only. Each company's compliance needs are different and "template" compliance programs must be conformed to the company's unique circumstances.

1. Key Elements

- Management Policy
- Responsible Officials
- Statutes and Regulations
- Recordkeeping
- Training
- Internal Reviews or Audits
- Notifications Mechanisms

2. Element-By-Element Summary

- Management Policy
    - Must outline and emphasize senior management's commitment to compliance with all applicable laws and regulations.
    - Must emphasize the significance of laws and regulations governing the company's international business.
    - Must be communicated to all levels within the company.
    - Must come from senior company management directly.
    - Must notify company employees of their obligations and the disciplinary consequences of failure to satisfy those obligations.

- Responsible Officials
    - Company must designate specific, readily identifiable individuals as *focal points* responsible for company compliance.
    - Sales personnel should not be designated as *focal points* (i.e., the export manager and the director of sales should be different people).
    - The *focal points* must be knowledgeable and well-trained in all facets of applicable laws and regulations.
    - The *focal points* should be identified by position, office, and telephone numbers.
    - The identification of *focal points* must be communicated to all levels within the company.

- Statutes and Regulations
    - Export Administration Act of 1979, as amended by the Omnibus Trade & Competitiveness Act of 1988, as amended (1993), 50 U.S.C. app. §§ 2401-2420 ("EAA") [N.B. Continued under the International Emergency Economic Powers Act ("IEEPA")].
        - National security controls
        - Foreign policy controls
        - Short supply controls
        - Controlled through licensing scheme
        - Administered by the Department of Commerce

- Export Administration Regulations, 15 C.F.R. part 730 et seq. (1997) ("EAR").
    - Implement export policies
        - General Prohibitions
        - Foreign policies
    - Authorizations to export
        - License exceptions
        - Licenses
        - Special comprehensive licenses
        - NLR - No License Required
    - Antiboycott Regulations, 15 C.F.R. Part 760
        - Preclude U.S. person's participation in any aspect of a transaction which furthers a boycott against nations friendly to the U.S.
        - Require separate reporting requirements
    - Re-export controls
    - Special country policies
    - Enhanced Proliferation Control Initiative
    - Other nuclear, chemical and biological weapons controls
    - Enforcement
        - What actions violate the EAA/EAR
        - Administrative procedures
        - Voluntary self-disclosures regarding violations
        - Mitigation
        - Criminal prosecution
    - Penalties
        - Suspension of export privileges
        - Civil fines

        - Criminal fines
        - Forfeitures
        - Seizures
        - Suspension/debarment from government contracts
        - Jail terms

- *Arms Export Control Act*, 22 U.S.C. §§ 2778-2994 ("AECA")
    - Foreign policy controls
    - National security controls
    - Control the export of:
        - Defense articles
        - Defense services
        - Controls administered through the Department of State

- International Traffic in Arms Regulations, 22 C.F.R. part 120 et seq. (1997) ("ITAR")
    - Implement export policies
    - Licensing scheme
        - Licenses
        - Agreements
        - Exemptions
    - Export and re-export controls
    - Recordkeeping requirements
    - Reporting requirements
    - Registration requirements
    - Screening requirements
    - Acquisition/divestiture requirements

- Proscribed country policies
- Coordination with OFAC Part 505 requirements
- Enforcement
  - What actions violate the AECA/ITAR
  - Administrative procedures
  - Voluntary self-disclosures regarding violations
  - Mitigation
  - Criminal prosecution
- Penalties
  - Suspension of export privileges
  - Civil fines
  - Criminal fines
  - Forfeitures
  - Seizures
  - Suspension/debarment from government contracts
  - Jail terms

- International Emergency Economic Powers Act, 50 U.S.C. § 1701 et seq. ("IEEPA")
  - Embargoes issued before 1977 enactment of IEEPA are based on the *Trading with the Enemy Act*, 50 U.S.C. app. §§ 1-44 ("TWEA").
  - Authorizes the President to institute embargoes against countries whose policies are anathema to U.S. interest or policies.
  - Treasury Department administers embargoes to specific destinations, e.g., Cuba, North Korea, Iran, Syria, and Sudan.

■ Recordkeeping

- Required by most applicable regulatory regimes.

- Must maintain records in an accurate and consistent manner, readily available for inspection by U.S. Government.
- Maintained for a minimum of years or as otherwise directed Administrative records, examples:
    - Department of Commerce
    - Department of State
    - Department of Treasury
    - Department of Justice
    - Securities and Exchange Commission
- Regulatory records, examples:
    - Current copies of all regulations and all updates
    - Current copy of the tables of denied parties and Federal Register updates
    - Records reflecting use of license exceptions
    - Records reflecting use of exemptions
- Transaction records, examples:
    - Invoices
    - Contracts, negotiation instruments, addenda, notes, memoranda, and other similar documents
    - Telefaxes or telegrams reflecting the transactions
    - Shipper's Export Declaration and other Customs documents
    - Air way bills/bills of lading

■ Training

- Continuous
- Current
- Targeted to employees based upon their responsibilities
- Regularly scheduled

- Clearly designated training individual(s)

■ Internal Review and Audits

- Designed to verify company compliance with its compliance system and all applicable laws
- Company-wide, including all divisions, branches, units or subsidiaries
- Clearly designated responsible official within the company or outside counsel to conduct the reviews
- Must be conducted annually, *at a minimum*
- Involves document reviews, personnel interviews, recordkeeping analysis, and preparation of internal systems review
- Reports; methodology used depends upon audit objectives: procedures review, investigation, due diligence review, or acquisition

■ Notification Mechanisms

- To consult with outside counsel or appropriate U.S. Government agency if questions arrive related to specific transactions
- To respond to enforcement inquiries
- To respond to anti-boycott requests
- To prepare voluntary self-disclosures to appropriate U.S. Government Agency
- To reasonably verify end-uses and/or end users.

X. About the Author

Mr. Kearney has over thirty years' experience representing clients in matters involving government and international contracting, regulatory compliance, internal investigations, and enforcement proceedings. His practice focuses on helping clients understand and manage the unique risks involved in global marketplaces and supply chains, including export and sanctions controls, anti-money laundering laws, anti-corruption regimes, and defense and national security issues. Mr. Kearney has handled numerous corporate due diligence reviews, internal investigations, prior disclosures, and resulting enforcement proceedings. He is a member of the Firm's Government Contracts Group, Global Practice Group, and Supply Chain Initiative, and represents regulated entities in the government contracting, export/import, financial, pharmaceutical, life sciences, defense, electronics, technology, and university/research sectors.

Mr. Kearney gratefully acknowledges the invaluable assistance of Stephen W. Cave, an attorney with Womble Carlyle, and Mark Thom, a summer associate with Womble Carlyle now attending the University of Virginia School of Law.

Mr. Kearney can be reached at JKearney@wcsr.com.

XI. Additional Resources

A. ACC Sources

"Top Ten Key Questions for Complying with United States Export and Embargo/Sanctions Law and Regulations," ACC Quick Reference (July 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=116689

B. Publications and Periodicals

Root, William A. et al., *United States Export Controls*, Fifth edition, New York, Aspen Publishers, 2000.

Corporate Counsel's Guide to Export Controls, 2d edition, West Group, 2005.

Export Today, 733 15th Street, N.W., Suite 1100, Washington, D.C. 20005, tel.: 202/737-1060, fax: 202/783-5966.

Foreign Trade Magazine, 6849 Old Dominion Drive, #200, McLean, VA 22101, tel.: 703/448-1338, fax: 703/448-1841.

Global Trade Magazine, North American Publishing Company, 401 North Broad Street Philadelphia, PA 19108, tel.: 215/238-5300.

International Business Magazine, American International Publishing Corporation, 500 Mamaroneck Avenue, Suite 314, Harrison, NY 10528, tel.: 914/381-7700, fax: 914/381-7713.

Inside International Trade, 1919 South Eads Street, Suite 201, Arlington, VA 22202, tel.: 1-800-424-9068 or 703-416-8505, fax: 1-703-416-8543, e-mail: insidetrade@iwpnews.com; online at World Trade Online (http://insidetrade.com)

International Trade Reporter, BNA, Inc., 9435 Key West Ave., Rockville, MD 20850

(800) 372-1033 (U.S. and Canada), (703) 341-3500 (International callers), fax: 1-800-253-0332, e-mail: customercare@bna.com .

International Trade Today, Broker Power, Inc., 7000 Infantry Ridge Road, Suite 104, Manassas, VA 20109, tel.: 800/524-5656, fax: 703/257-7700, e-mail: sales@brokerpower.com.

The Exporter, 34 West 37th Street, New York, NY 10018, tel.: 212/563-2772, fax: 212/563-2798.

The Export Practitioner, Gilston-Kalin Communications, P.O. Box 5325, Rockville, MD 20848-5325, tel: 202/463-1250, fax: 202/429-9812.

C. Online Resources

Arms Control Association: http://www.armscontrol.org/

Bureau of Industry and Security, U.S. Department of Commerce: http://www.bis.doc.gov/

Customs & Border Protection, U.S. Homeland Security Department: http://www.customs.gov/

Directorate of Defense Trade Controls, U.S. Department of State: http://www.pmddtc.state.gov/

Office of Foreign Assets Control, U.S. Department of Treasury: http://www.treas.gov/offices/enforcement/ofac/

XII. Endnotes

[1] Although not the "exporter of record", a U.S. person transferring possession, control or ownership of a dual-use article to any other person in the United States could be held accountable for an unlawful export by that person to the extent s/he conspired in the unlawful export or transferred the article knowing that the export would violate the EAR.

[2] The Export Administration Regulations use the term "foreign national"; the International Traffic in Arms Regulations use the term "foreign person." However, they are defined the same way.

[3] The United States federal agencies with export control responsibilities are set forth at EAR Part 730, Supplement No. 3.

[4] 15 C.F.R. Part 730 et seq.

[5] 50 U.S.C. App. §§ 2401 et seq. Although the EAA expired in 1994, the EAA and the EAR remain in effect through annual executive orders issued pursuant to the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-1706.

[6] 22 C.F.R. Part 120 et seq.

[7] 22 U.S.C. § 2278.

[8] 22 C.F.R. § 121.1.

[9] 31 C.F.R. Part 500 et seq.

[10] 50 U.S.C. § 1701 et seq.

[11] 50 U.S.C. App. §§ 1 et seq.

[12] 22 C.F.R. § 120.5

13 See the BIS Interactive Tool at http://beta-www.bis.doc.gov/index.php/export-control-classification-interactive-tool

[14] 15 C.F.R. § 734.3.

[15] The ten Commerce Control List categories have been assigned numbers beginning with "0" and ending with "9".

[16] Denied person screening can be done internally if appropriate resources are devoted to the effort. Alternatively, there are a variety of vendors providing screening services and access to updated screening lists on an outsourced basis,

[17] On August 26, 2013, DTC published an interim final rule amending the ITAR with respect to brokers and brokering activities. The effective date of the rule is October 25, but comments will be accepted until October 10, with a "final" rule published reflecting any additional revisions. Unless the interim final rule is further revised, the rule would broaden the definitional scope of "brokering activities" in Part 129 to include "any action on behalf of another to facilitate the. . .transfer, reexport, or retransfer. . .of a defense article." In addition, the rule would remove from the definitional scope of "broker" any foreign person not located in the U.S. and not owned/controlled by a U.S. person.

[18] ITAR § 120.6.

[19] ITAR Section 120.9. At the time of publication, a proposal is pending to revise the definition of "Defense Services" to focus more specifically on the forms of assistance covered by that term.

[20] See No. xiv.

[21] See No. xiv.

[22] See No. xv.

[23] Department of Defense Federal Acquisition Regulation Supplement 252.204-7008.

[24] Federal Acquisition Regulation 52.225-13.

[25] Malaysia's Strategic Trade Act of 2010 ("STA") exemplifies efforts by countries to control the export, transit and brokering of technology including arms and activities that could facilitate the design, development, production and delivery of weapons of mass destruction.

[26] Brazil amended its KYC laws in 2012 to outlaw transactions with individuals and companies designated on various lists found on Brazil's government websites.

[27] In 2012, Vietnam passed its first anti-money laundering law, requiring financial institutions to verify clients' information in certain transactions.

[28] ITAR §120.7 denotes significant military equipment to mean articles for which special export controls are warranted because of their capacity for substantial military utility or capability; see also ITAR §126.8