

BRIEFING PAPERS

SECOND SERIES



PRACTICAL TIGHT-KNIT BRIEFINGS INCLUDING ACTION GUIDELINES ON GOVERNMENT CONTRACT TOPICS

DUE DILIGENCE & COMPLIANCE RISK MANAGEMENT ABROAD FOR GOVERNMENT CONTRACTORS

By Andrew D. Irwin, Negar Katirai, and David S. Lorello

Developments of the past several decades, including an increase in U.S. military deployments abroad, have resulted in more U.S. Government contractors operating internationally. The rise of contingency support work and service contracts abroad has drawn U.S. companies to provide their goods and services first in the Balkans and now primarily in Afghanistan and Iraq, as well as for related in-theater operations. Indeed, as a result of current operations in Iraq and Afghanistan, there are exponentially more contractors supporting U.S. and allied military forces than ever before.¹ Similarly, foreign military sales and foreign direct contracts continue to serve as a growth engine, albeit sporadically, for U.S.

Government contractors. At the same time, other trends, including the war on terrorism, nuclear proliferation, changes in U.S. and multilateral export controls, and heightened awareness of and enforcement activity regarding public corruption, have resulted in a more complex legal and regulatory structure for Government contractors operating abroad. These companies must not only manage sometimes unfamiliar commercial, political, and legal environments in other countries but must also concurrently maintain compliance with U.S. laws and regulations, including those implemented to prevent U.S. companies from engaging in foreign bribery, to prevent military and dual-use goods and technology from reaching the hands of terrorist networks or other improper end users or end uses, and to counter the boycott of Israel by some members of the Arab League.

IN BRIEF

- | | |
|-------------------------------|--|
| Foreign Corrupt Practices Act | Antiboycott Rules |
| ■ Scope | ■ Compliance |
| ■ Penalties | ■ Penalties |
| ■ Enforcement | |
| Money Laundering Control Act | Know Your Government Customer |
| ■ Scope | ■ U.S. Government Customer Issues |
| ■ Penalties | ■ Foreign Government Customer Issues |
| U.S. Economic Sanctions | Know Your Partner |
| ■ Scope | ■ U.S. Peer Group Companies |
| ■ Iran | ■ Foreign Peer Group Companies |
| ■ Sudan | ■ Smaller U.S. Companies |
| ■ Syria | ■ Smaller Foreign Companies Or Non-Peer Group Entities |
| ■ Other Sanctions Programs | ■ Minority Partnership |
| U.S. Export Controls | Know Your Third-Party Representatives |
| ■ ITAR | |
| ■ EAR | |
| ■ ITAR Compliance | |
| ■ EAR Compliance | |
| ■ Enforcement | |
| ■ Penalties | |
| | Know Your Subcontractor |
| | ■ U.S. Companies |
| | ■ Foreign Companies |

Andrew D. Irwin is Special Counsel in Steptoe & Johnson LLP's Government Contracts Group, as well as its International Regulations and Compliance Group in Washington, D.C. Negar Katirai and David S. Lorello are associates in the firm's International Regulations and Compliance Group, practicing in Washington and London, respectively.

This BRIEFING PAPER presents an overview of the most important legal regimes implicating due diligence and compliance risk management concerns for U.S. Government contractors operating abroad, including the Foreign Corrupt Practices Act, anti-money laundering laws, economic sanctions and export control regulations, and antiboycott regulations. In addition, this PAPER highlights the major risk areas to be considered and precautions to be taken when dealing with customers, teaming partners, third-party representatives, and subcontractors abroad. Because there are countless rules that apply to such scenarios,² this PAPER focuses on the most pressing due diligence issues at an overview level. Companies are urged to carefully consider—and to seek advice when necessary regarding—the legal and regulatory issues highlighted here, as well as other potentially applicable laws and regulations that may affect their business operations abroad.

Foreign Corrupt Practices Act

The U.S. Foreign Corrupt Practices Act (FCPA)³ contains broad prohibitions against any act “in furtherance of” bribery of foreign public officials to obtain or retain business by U.S. persons or companies, by “issuers” of U.S. securities whether incorporated in the United States or elsewhere, and by “any person” acting on U.S. territory.⁴ The concept of “obtaining or retaining business” in the FCPA has been interpreted broadly to include obtaining not only foreign government contracts, but also government-provided advantages that are incidental to doing business in foreign countries, such as customs and tax benefits.⁵ The term “foreign official” is also expansive.⁶

In addition to its antibribery provisions, the FCPA mandates that issuers implement record-keeping, internal accounting controls, and other measures, at the parent and subsidiary level, to ensure that the company’s books and records do not disguise or conceal improper payments.⁷ For a nonmajority-owned or -controlled affiliate, the parent’s obligation is to use good faith efforts to cause that affiliate to implement the books and records obligations.⁸

■ Scope

FCPA jurisdiction is based in part on *nationality*, in that “U.S. persons” (a defined term that encompasses both U.S. companies and U.S. nationals or permanent residents⁹) are subject to the FCPA regardless of where the bribery takes place, and also on *territoriality*, meaning that the activities of non-U.S. persons could be subject to the FCPA if there is a sufficient nexus between a person’s conduct and the United States. The latter concept has been interpreted expansively by U.S. enforcement officials: the linkage between a person’s actions and the United States may be as minimal as the use of the U.S. mails, telephone system, or other facilities in U.S. interstate commerce or actions within the United States that further a substantive violation. In some cases, foreign persons have been prosecuted for acts occurring wholly outside the United States that were intended to affect conduct within the United States.¹⁰

■ Penalties

Violations of the FCPA antibribery provisions and accounting provisions are subject to a range of penalties, which are assessed on a per-violation



BRIEFING PAPERS

This publication was created to provide you with accurate and authoritative information concerning the subject matter covered; however, this publication was not necessarily prepared by persons licensed to practice law in a particular jurisdiction. The publisher is not engaged in rendering legal or other professional advice, and this publication is not a substitute for the advice of an attorney. If you require legal or other expert advice, you should seek the services of a competent attorney or other professional.

BRIEFING PAPERS® (ISSN 0007-0025) is published monthly except January (two issues) and copyrighted © 2007 ■ Valerie L. Gross, Editor ■ Periodicals postage paid at St. Paul, MN ■ Published by Thomson/West / 610 Opperman Drive, P.O. Box 64526 / St. Paul, MN 55164-0526 ■ <http://www.west.thomson.com> ■ Customer Service: (800) 328-4880 ■ Postmaster: Send address changes to Briefing Papers / PO Box 64526 / St. Paul, MN 55164-0526

BRIEFING PAPERS® is a registered trademark used herein under license. All rights reserved. Reproduction, storage in a retrieval system, or transmission of this publication or any portion of it in any form or by any means, electronic, mechanical, photocopy, xerography, facsimile, recording or otherwise, without the written permission of Thomson/West is prohibited. For authorization to photocopy, please contact the Copyright Clearance Center at 222 Rosewood Drive, Danvers, MA 01923, (978)750-8400; fax (978)646-8600 or West’s Copyright Services at 610 Opperman Drive, Eagan, MN 55123, fax (651)687-7551.

basis but can rise to tens of millions of dollars in total penalties. With regard to the antibribery provisions, companies are subject to criminal fines of up to \$2 million and civil fines of up to \$10,000 per violation.¹¹ Individuals violating the antibribery provisions are subject to civil fines of up to \$10,000 per violation¹² and criminal penalties of up to \$250,000 per violation and/or five years' imprisonment.¹³ Companies and individuals are also subject to penalties of twice the amount of the pecuniary gain resulting from the FCPA violation.¹⁴ Companies may not reimburse officers, directors, employees, agents, or stockholders the cost of any fines imposed on them.¹⁵

Violations of the FCPA's recordkeeping and internal accounting controls provisions can result in civil penalties per violation of up to the greater of \$500,000 for companies and \$100,000 for individuals or up to twice the amount of any pecuniary gain resulting from the violation.¹⁶ Criminal penalties can include fines of up to \$5 million per violation and imprisonment for up to 20 years for individuals and fines of up to \$25 million per violation for companies.¹⁷

In addition to monetary penalties and the risk of incarceration, parties that violate the FCPA may be subject to a range of other parallel sanctions, including suspension or debarment from public contracting¹⁸ and denial of U.S. export or import license requests,¹⁹ and may face difficulties in obtaining contracts funded by international financial institutions (such as the World Bank).

■ Enforcement

The U.S. Department of Justice and the Securities and Exchange Commission, which are tasked respectively with criminal and civil enforcement authority for antibribery and accounting violations, enforce the FCPA aggressively. Enforcement has increased substantially since 1998, when the FCPA was amended to broaden its jurisdictional scope,²⁰ and in wake of the various corporate accounting scandals in the United States and abroad in recent years. By way of recent example, in May 2007, corporate affiliates of Baker Hughes Inc. agreed to pay a total of \$44.1 million, including criminal fines, civil penalties, and disgorgement of profits, the highest penalty in an FCPA case to date.²¹

While the FCPA itself spawned from foreign government contracts in the 1970s, recent FCPA enforcement actions have also occurred in contingency U.S. Government contracting environments, including the war in Iraq. For example, in one recent case, a naturalized U.S. citizen of Iraqi descent working for Titan Corporation as a translator in Iraq was sentenced to three years in prison for violating the antibribery provisions of the FCPA by offering a senior official with the Iraqi police force a bribe to induce the official to use his position to facilitate the proposed procurement of a map printer and 1,000 armored vests.²²

Finally, it should be kept in mind that non-U.S. local antibribery and commercial antibribery laws could apply to impose liability irrespective of the presence or absence of FCPA jurisdiction. These laws sometimes define the concept of "bribery" more broadly (or less precisely) than the FCPA, thus making it important for companies to develop a clear understanding of foreign local legal issues as part of the company's broader anticorruption compliance efforts.

Money Laundering Control Act

The U.S. Money Laundering Control Act (MLCA)²³ establishes liability for individuals and entities that conduct transactions knowing that the proceeds involved were derived from unlawful activity or with the intent to promote some unlawful activity. The statute sets forth three types of prohibitions: (1) "transactional money laundering," where the financial transaction itself is prohibited because it involves the proceeds of some form of unlawful activity,²⁴ (2) "transportational money laundering," where transport of funds into or out of the United States is prohibited regardless of whether a financial transaction with another party occurs,²⁵ and (3) a "trafficking" prohibition criminalizing the receipt of criminally derived property that has a value greater than \$10,000.²⁶

■ Scope

Because the MLCA now includes FCPA violations and other bribery-related offenses as predicate offenses (termed "specified unlawful activities"),

as well as certain export-related offenses,²⁷ money laundering charges, particularly charges based on the transportation provision of the MCLA, are often asserted in FCPA prosecutions. Indeed, the statute is expansive in scope and can be used by U.S. enforcement authorities with respect to conduct that occurs predominately abroad. Therefore, money laundering and the FCPA are often inexorably intertwined.

■ Penalties

Violations of the transactional and transportation money laundering provisions of the MLCA are punishable with fines of up to \$500,000 or twice the value of the property involved in the transaction, whichever is greater, as well as imprisonment for up to 20 years.²⁸ Violations of the trafficking provision of the MLCA are punishable by fines of between \$5,000 and \$250,000, depending on how the criminal violation is classified, or twice the amount of the criminally derived property involved in the transaction, as determined by judicial discretion, as well as imprisonment for up to 10 years.²⁹

U.S. Economic Sanctions

The United States maintains economic sanctions against certain countries and entities for foreign policy reasons. Sanctions are administered by the U.S. Department of the Treasury's Office of Foreign Assets Control³⁰ and are promulgated pursuant to the International Emergency Economic Powers Act (IEEPA),³¹ the Trading With the Enemy Act,³² and related Executive Orders issued by the President pursuant to these statutes. OFAC has civil enforcement authority over sanctions violations, whereas the DOJ handles criminal prosecutions.

■ Scope

The OFAC sanctions restrictions apply for the most part to "U.S. persons," a term defined to include U.S.-incorporated entities and their foreign branches, U.S. permanent residents, and foreign persons located in the United States.³³ Certain provisions in the sanctions regulations—in particular, restrictions relating to the transfer of U.S.-origin goods from foreign locations to

sanctioned countries—also apply to foreign persons.³⁴

In most of the sanctions programs, the restrictions applicable to "U.S. persons" do not apply to independently operating foreign subsidiaries of U.S. companies, though certain sanctions programs (such as those restrictions regarding Cuba)³⁵ extend in full to independent foreign subsidiaries. Nevertheless, the OFAC regulations include broad restrictions that prohibit "U.S. persons" from taking any action to "facilitate" or "approve" business by foreign persons with sanctioned countries (even if the foreign persons are not themselves subject to OFAC restrictions). This could include activities such as referring sanctioned-country business opportunities to corporate affiliates or third parties or providing internal corporate approvals for specific sanctioned-country transactions undertaken by foreign affiliates.³⁶

Currently, the United States maintains broad-based economic embargoes against Cuba,³⁷ Iran,³⁸ and Sudan.³⁹ OFAC also administers more targeted economic sanctions against Burma (Myanmar),⁴⁰ and Syria is subject to wide-ranging export controls, though those restrictions are administered by the Department of Commerce rather than OFAC. OFAC also publishes a list of companies and individuals, known as the Specially Designated Nationals (SDNs) and Blocked Persons List, who are sanctioned for their connections with targeted countries, terrorists, or narcotics traffickers.⁴¹ The Department of State also publishes a shorter list of terrorist organizations,⁴² and there is another list of entities subject to multilateral United Nations sanctions.⁴³ Those wishing to deal with sanctioned countries or entities must request a specific license from OFAC, which generally will not be granted unless unique circumstances are present that render the transaction clearly supportive of U.S. national security interests.⁴⁴

■ Iran

U.S. sanctions against Iran have been in place since 1987⁴⁵ and were substantially expanded in the mid-1990s as a result of Iran's continuing pursuit of a nuclear weapons program and its support of designated international terrorists. The Iran sanctions regulations prohibit U.S. persons,

wherever located, from participating in virtually all trade and investment activities with Iran, including exporting or reexporting U.S.-origin goods, services, or technology to Iran, importing most Iranian-origin goods and services, and “facilitating” business of third-country nationals or companies with Iran.⁴⁶

As of spring 2007, both houses of Congress are currently considering separate legislation imposing additional sanctions on Iran, including expanding the sanctions to independently operating U.S. subsidiaries.⁴⁷ Iran has also recently been subject to a wide range of multilateral sanctions through the U.N. Security Council. These sanctions, which are being implemented by U.N. members states through national legislation, include a wide range of prohibitions on doing business in the Iranian nuclear and military sectors.⁴⁸

Contractors need to be particularly mindful of Iran sanctions, as they could hire subcontractors that may wish to source product from Iran, ship items through Iran, or use representative offices in Iran. All of these actions would represent potential violations of U.S. law and create potential compliance issues for higher-tier U.S. contractors.

■ Sudan

Sudan is also listed by the State Department as a state sponsor of terrorism and is the subject of a broad-based U.S. embargo.⁴⁹ In November 1997, President Clinton issued an Executive Order imposing a trade embargo against Sudan and a total asset freeze against the Government of Sudan.⁵⁰ These sanctions, which largely parallel the sanctions applicable to Iran, prohibit U.S. persons from importing goods or services from Sudan, from exporting goods, technology, or services to Sudan, and from engaging in financial transactions in Sudan. Like the Iran sanctions, these prohibitions include exports by U.S. persons to a third country with the knowledge that such items will be reexported to targeted countries or otherwise “facilitating” business by third-country nationals with Sudan.⁵¹ The sanctions against Sudan do not, however, apply to activities or related transactions with respect to Southern Sudan, including Darfur and other

specified areas, where the activities or transactions in question do not involve any property or interests in property of the Government of Sudan, although all petroleum-related transactions are still subject to controls.⁵² To the extent that U.S. contractors support U.S. Government assistance efforts regarding Sudan, they need to be mindful of potential OFAC licensing implications.

■ Syria

President Bush signed the Syria Accountability and Lebanese Sovereignty Restoration Act in December 2003 to impose a broad set of export controls on Syria, which is also listed by the State Department as a state sponsor of terrorism.⁵³ Aside from sanctions applying to transactions with SDNs, these sanctions are administered by the Department of Commerce rather than OFAC.⁵⁴

The Syria restrictions ban the export or reexport to Syria of virtually all U.S.-origin goods and technology, although certain limited subsets of goods can be licensed by the Commerce Department for export or reexport on a case-by-case basis.⁵⁵ In contrast to the OFAC-administered trade restrictions applicable to Iran and Sudan, the Syria restrictions generally do not prohibit U.S. persons from doing business in or providing commercial services to Syria, provided that the use of restricted U.S. goods or technology is not involved.⁵⁶

As in the case of the Iran restrictions, contractors need to be aware, for instance, of shipments of U.S.-origin goods that might transit through Syria. It is important, therefore, to ensure that all subcontractors at all tiers are aware of Syria-related restrictions.

■ Other Sanctions Programs

Until recently, Iraq and Libya had been subject to long-standing U.S. economic embargoes similar to the restrictions currently applicable to Iran. In recent years, however, those sanctions have been lifted. Libya and Iraq are now subject to a more or less standard set of export controls restrictions administered by the Department of Commerce, largely similar to those applicable to other countries in the region such as Jordan and Kuwait, though there are certain nuclear proliferation and military arms

restrictions that are stronger than for most other countries in region.⁵⁷ It should be noted, however, that a large number of SDNs and blocked persons continue to operate in Iraq and Libya. It is essential, therefore, to run names of entities against the SDN list when doing business in or with those countries. North Korea also had previously been subject to broad-based sanctions restrictions, but those also largely have been lifted, although OFAC retains restrictions on imports from North Korea, and a variety of North Korean entities are designated as SDNs.⁵⁸ Moreover, exports to North Korea are subject to very stringent licensing requirements under the Department of Commerce-administered Export Administration Regulations (discussed below).⁵⁹

As noted above, Burma is also subject to U.S. economic sanctions, though those sanctions are more targeted than with regard to Cuba, Iran, and Sudan. A series of statutes, regulations, and Executive Orders collectively prohibit the import of Burmese products, new investment activity in Burma, and the export of financial services to Burma from the United States and also freeze the assets of designated entities and individuals in Burma.⁶⁰

Finally, OFAC retains residual sanctions regulations relating to other countries, such as Afghanistan and the Balkans, but those restrictions at this point are limited to prohibiting dealings with SDNs (such as designated Taliban-supporting entities in Afghanistan).⁶¹

U.S. Export Controls

Companies shipping commodities, technology, and software abroad must comply with U.S. export controls, which are administered by the Department of State and the Department of Commerce. Companies exporting nuclear and nuclear-related items may also be subject to export controls administered by the Department of Energy and the Nuclear Regulatory Commission.⁶²

■ ITAR

The Department of State's Directorate of Defense Trade Controls administers the International Traffic in Arms Regulations,⁶³ which are promul-

gated under the Arms Export Control Act.⁶⁴ The DDTTC regulates the export of "defense articles," "technical data," "defense services," and "brokering" of defense transactions. These terms are interpreted broadly by the DDTTC to cover many types of goods and services that are conventionally considered not specific to the military but that have some military element to them.⁶⁵ In addition, the DDTTC requires registration of U.S. defense manufacturers and exporters, as well as brokers,⁶⁶ and restricts payment of commissions or fees in securing defense business.⁶⁷ The ITAR apply to "U.S. persons" (defined to include lawful permanent residents as well as any corporation or other entity incorporated in the United States) and to foreign persons in possession of ITAR-controlled goods or technical data that are of U.S. origin.⁶⁸

■ EAR

The Department of Commerce's Bureau of Industry and Security administers the Export Administration Regulations,⁶⁹ which are promulgated under the Export Administration Act⁷⁰ and the IEEPA.⁷¹ The EAR are the principal regulatory framework for controlling exports and reexports of U.S.-origin goods and technology. Although BIS has regulatory authority over all U.S.-origin items, the EAR generally impose export licensing requirements only for a specified subset of goods known generally as "dual-use" items (because they have potential military in addition to commercial applications or otherwise are of a technical capability that poses unique national security risks).⁷² For some of the sanctioned countries noted above (such as Iran, Syria, Sudan, and Cuba) and for certain designated entities, the EAR impose broader license requirements on non-dual-use items.⁷³ Like the ITAR, the EAR apply to U.S. persons and to foreign persons in possession of U.S.-origin goods or technology (whether in the United States *or abroad*).⁷⁴

■ ITAR Compliance

Under the ITAR regime for regulating the export of defense-related items, companies shipping potentially military-controlled items or technical data abroad must review the U.S. Munitions List (USML), which lists the items controlled under the

ITAR.⁷⁵ The USML is separated into 21 categories, such as guns and armament, aircraft and associated equipment, military electronics, and toxicological agents.⁷⁶ The USML includes, notably, a “catch-all” provision that controls any item not otherwise specified in the USML that has been “specifically designed” for a military end use.⁷⁷ This provision has been interpreted broadly by the DDTC, and it can capture many items that are conventionally understood to be nonmilitary but that the DDTC treats as ITAR-controlled because they have been modified in some way for a military end use (even if the modification is relatively insignificant). All items and technical data listed in the USML require a license from the DDTC for export unless a license exemption applies.⁷⁸

One substantial difference between the EAR and the ITAR is that the ITAR regulate services in addition to goods and therefore require parties (in many cases) to receive prior authorization from the DDTC before providing defense services. To receive DDTC approval for defense services, parties must submit draft “manufacturing license agreements” and “technical assistance agreements” to the DDTC, which must specify the terms of the services to be provided.⁷⁹ The process for approving these agreements can often take many months. (It is not surprising for a proposed agreement to remain pending at the DDTC for nine months or longer.) Therefore, parties engaged in ITAR-related activities must plan well in advance to ensure that all necessary DDTC authorizations are in place by the time work begins. Technical assistance agreements in particular have been important to many multinational defense efforts, where the subcontractor base has involved numerous contractors from other countries.

Certain exemptions exist for U.S. Government programs abroad. For example, temporary exports sent for or by the use of the U.S. Government can be exempt (subject to certain preconditions set forth in the ITAR), as are certain technical data shipments under certain Government contracts or certain shipments of technical data to U.S. person employees of the U.S.-incorporated exporting company.⁸⁰ Likewise, there are instances in which a DOD official can order that certain transactions be exempt from ordinary licensing procedures,

though many contractors may misperceive the DOD’s ability and authority to effectively issue such orders.⁸¹ It is essential that U.S. contractors abroad not automatically assume that just because their work is for the U.S. Government they do not need to be concerned with export controls. While in many instances contractors will be able to use exemptions, given that the DDTC may read exemptions narrowly, it is important to carefully assess the scope of the exemptions.

It is also important to be aware that even when a contractor is not engaging in a program that itself results in the production of an ITAR-controlled item, various equipment and tools that a contractor uses in the course of its work may be ITAR controlled. For example, certain protective equipment is controlled.⁸² Likewise, contractors must realize that the ITAR contain outright arms embargoes for certain countries, e.g., China.⁸³ Taking equipment to or through such countries, even incidentally, or exposing technology to nationals of those countries in the course of your work could have significant consequences.

■ EAR Compliance

Because items controlled under the EAR often are relatively low technology and/or are widely available for commercial purchase around the world, many companies overlook their EAR compliance obligations. EAR license requirements could apply to many products ordinarily used in Government contracting environments, such as high-performance computers and software, personnel security equipment (though some may be ITAR controlled), certain high-performance building materials, and various other goods that fall within specific categories of the EAR Commerce Control List (CCL).⁸⁴ The EAR also control blueprints, design plans, and other technical information associated with these products.⁸⁵

In addition to regulating exports from the United States, the EAR control the “reexport” of certain U.S.-origin items between non-U.S. jurisdictions (including by foreign persons) and the export of foreign-made items with U.S.-origin content.⁸⁶ Moreover, the EAR regulate the sharing of U.S.-origin technical data with a foreign national who is not a permanent resident alien, even if that person is in the United States and employed by

a U.S. company under an appropriate work visa. This is known as a “deemed export.”⁸⁷

Thus, the manner of export is not significant to determining BIS jurisdiction, as BIS has jurisdiction over any item transferred outside the United States, whether it is shipped, mailed, faxed, or sent via e-mail over the internet.⁸⁸ Furthermore, even items that leave the United States temporarily or are transferred to U.S. subsidiaries located abroad are considered exports and could be subject to EAR license requirements.⁸⁹ Companies must also assess whether the product is restricted for export or reexport to the intended end user—both BIS and OFAC maintain lists of persons who are restricted from receiving U.S.-origin goods or technologies. (The OFAC SDN list is discussed above⁹⁰; separately, BIS maintains the “Denied Persons List” and “Entity List,” which impose separate and independent restrictions on certain entities.⁹¹)

Companies new to navigating the often complex and intricate EAR regulations may find the “Export Control Basics” page on BIS’s website to be a helpful starting point.⁹² Likewise, companies and their compliance staffs may find that flowcharts included within the EAR serve as helpful “decision trees.”⁹³ While there are various license exceptions (e.g., License Exception GOV, which applies to exports to government entities, including certain foreign governments)⁹⁴ or programs such as the Special Iraq Reconstruction License⁹⁵ that may apply for certain Government contracting programs, contractors may fail to take into account the specific requirements necessary to qualify for such exceptions or programs and, instead, merely assume that they apply.

■ Enforcement

In general, there has been a significant increase in both civil and criminal EAR and OFAC enforcement cases. BIS and OFAC have traditionally targeted Iran- and Cuba-related infractions for investigation and assessment of penalties, and there has been a mounting focus on exports to China and the Middle East.⁹⁶ The EAR contain strict regulations for many Middle Eastern countries, and, as a practical matter, many of these restrictions are increasingly relevant for Government contractors, given the heightened activity by such contractors in the Middle East and Southwest Asia. For example,

the EAR require a license for exports to Iraq for all reasons of control except most items controlled for antiterrorism purposes only,⁹⁷ and restrictions on dual-use items remains strict for Libya and many other countries in the region.⁹⁸ However, many licensing exceptions, including for temporary exports (License Exception TMP),⁹⁹ now apply to exports to those countries, and, as noted, contractors may now apply for a Special Iraq Reconstruction License to conduct reconstruction activities in Iraq.¹⁰⁰ In addition, because Syria is subject to a wide range of export and other restrictions, basically all items that are of U.S. origin or contain more than 10% U.S. content are restricted for export to Syria absent a license from BIS.¹⁰¹ Libya is still subject to a U.S. arms embargo, though limited defense articles are licensable for Libya under the ITAR.¹⁰² Significantly, BIS has sought to heighten awareness of U.S. export controls by creating an Arabic translation of its website primer “Export Control Basics.”¹⁰³ Other languages are now available as well.

■ Penalties

Penalties for violations of the EAR and OFAC regulations can take the form of criminal fines of up to \$500,000, or twice the pecuniary gain or loss of the transaction, as well as civil fines of up to \$50,000 per violation.¹⁰⁴ In addition, criminal penalties can include imprisonment for up to 20 years.¹⁰⁵ Penalties for violations of the ITAR can take the form of criminal fines of up to \$1 million and civil fines of up to \$500,000.¹⁰⁶ Criminal penalties can include imprisonment for up to 10 years.¹⁰⁷

In addition, violations of the EAR or the ITAR can result in nonmonetary sanctions such as the loss of export privileges¹⁰⁸ or suspension and debarment,¹⁰⁹ respectively. Companies also may be required to employ internal compliance monitors as part of settlement agreements.¹¹⁰ Moreover, both BIS and the DDTC publish information regarding violations and settlements, even in cases of voluntary disclosure.¹¹¹

Antiboycott Rules

In response to the Arab League boycott of Israel in the 1970s, Congress enacted laws to counteract the participation of U.S. citizens and companies in the Arab League and other boycotts. These laws

were included in the 1977 amendments to the Export Administration Act (EAA),¹¹² implemented in the EAR,¹¹³ and the Ribicoff Amendment to the 1979 Tax Reform Act (TRA).¹¹⁴ Both sets of rules are extremely complex and should be carefully studied by contractors operating abroad. By way of example, the Commerce Department regulations contain numerous hypothetical factual scenarios.

The EAR prohibit (1) refusals to do business with or in a boycotted country, (2) refusals to employ or other discrimination against any individual who is a U.S. person on the basis of race, religion, sex, or national origin, (3) the furnishing of information about the race, religion, sex, or national origin of any U.S. person, (4) the furnishing of information about business relationships with boycotted countries or blacklisted persons, (5) the furnishing of information concerning association with charitable or fraternal organizations that support boycotted countries, and (6) the implementation of letters of credit that contain prohibited conditions or requirements.¹¹⁵

The TRA does not prohibit any conduct but subjects to penalties certain participation in or cooperation with foreign international boycotts. For this purpose, a person participates in or cooperates with an international boycott if the person agrees, as a condition of doing business directly or indirectly within a country or with the government, a company, or a national of a country, to (a) refrain from doing business with or in a country that is the object of the boycott or with the government, companies, or nationals of that country, (b) refrain from doing business with any U.S. person engaged in trade in a country that is the object of the boycott or with the government, companies, or nationals of that country, (c) refrain from doing business with any company whose ownership or management is made up, all or in part, of individuals of a particular nationality, race, or religion, (d) remove (or refrain from selecting) corporate directors who are individuals of a particular nationality, race, or religion, or (e) refrain from employing individuals of a particular nationality, race, or religion.¹¹⁶ In addition, a person participates in or cooperates with an international boycott if

the person agrees, as a condition of the sale of a product to the government, a company, or a national of a country, to refrain from shipping or insuring that product on a carrier owned, leased, or operated by a person who does not participate in or cooperate with an international boycott.¹¹⁷

Currently, the Arab League boycott of Israel remains the primary boycott with which U.S. companies must be concerned. The U.S. Treasury Department publishes a quarterly list of boycotting countries. The most recent list, published April 2007, lists Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, the United Arab Emirates, and the Republic of Yemen.¹¹⁸ Iraq's status is under continued review by the U.S. Government.

■ Compliance

Both the EAR and TRA require individuals and companies to report requests regarding boycott compliance. The EAR require U.S. persons to report requests to comply with, further, or support a foreign boycott using Form BIS-621P for single transactions and Form BIS-6051P for multiple transactions received in the same quarter.¹¹⁹ The term "U.S. person" is defined to include foreign entities and branches that are "controlled in fact" by a domestic concern. "Control in fact" is the authority or ability of a domestic concern to establish the general policies or to control day-to-day operations of any foreign subsidiary, partnership, affiliate, branch, office, or other permanent foreign establishment. The EAR set forth a variety of specific criteria (including, among other things, corporate ownership and corporate governance authorities) that determine whether a foreign company is "controlled in fact" by a U.S. company.¹²⁰

In addition, all persons subject to the EAR must maintain records relating to transactions involving restrictive trade practices or boycotts, as well as those involving certain exports and certain other transactions subject to the rules. This requirement to maintain records generally applies to negotiations regarding transactions as well. The records to be kept include contracts, invitations to bid, financial records, books of account, memoranda, notes and correspondence, and any other boycott-related documents and reports.¹²¹

The TRA requires taxpayers to report “operations” in, with, or related to a boycotting country or its nationals, as well as requests to participate in or cooperate with an international boycott, with tax returns on IRS Form 5713.¹²²

■ Penalties

Violations of the TRA can include the denial of all or part of the foreign tax benefits discussed above. Penalties for violations of the EAR antiboycott regulations can include criminal fines of up to \$50,000 and imprisonment for up to 20 years for knowing violations and criminal fines of up to \$250,000 and imprisonment for up to 20 years for “willful” violations.¹²³ The criminal penalty for a corporation may include a fine of up to \$500,000 or twice the pecuniary gain or loss to the corporation.¹²⁴ Civil penalties can include fines of up to \$50,000 per violation and a general denial of export privileges, among other things.¹²⁵

Multiple violations may result in higher penalties. For example, in June 2000, the Department of Commerce imposed a \$104,000 civil penalty on Kenclaire (West) Electrical Agencies, Inc. to settle allegations that the company had violated the EAR antiboycott provisions on 11 occasions by agreeing not to do business with manufacturers boycotted by Saudi Arabia. The Department also alleged that Kenclaire committed 19 additional violations when it failed to report its receipt of requests to comply with boycott requests from Saudi Arabia.¹²⁶

Know Your Government Customer

■ U.S. Government Customer Issues

Doing work outside the United States poses many special challenges. In a contingency contracting environment, chains of command are often different from those in a domestic military or civilian agency context. As a result, contractors are increasingly faced with orders from military commanders rather than from Contracting Officers or agency officials themselves.

Contractors need to be aware of the complexity and challenges of such chain of command issues before deploying abroad. And they need to attempt,

as best they can, to document exactly to whom they report. Indeed, certain contractors are now subject to military extraterritorial criminal jurisdiction.¹²⁷

Civilian agency customers also present special challenges. For instance, when working for the U.S. Agency for International Development, contractors are subject to a complicated set of additional rules and regulations set forth in the AID Acquisition Regulation as a result of USAID’s need to comply with the Foreign Assistance Act.¹²⁸ These rules are known as “Source, Origin and Nationality.” Some of these rules overlap sanctions regulations but they also place further restrictions on the entities with which a contractor may subcontract (including the subcontractor’s country) and on items that may be purchased in certain contracting efforts.¹²⁹

■ Foreign Government Customer Issues

Foreign customers present special challenges. Among others, there may be significant export control restrictions, absent exceptions applicable to the Foreign Military Sales program.¹³⁰ U.S. Government contractors used to being able to invoke exemptions to the ITAR when working for the U.S. Government and in essence navigate around export controls must realize that a foreign customer presents a wholly new set of export control challenges. Such challenges need to be accounted for from a cost and schedule perspective at the time of bidding. Indeed, it is important to note that, under the ITAR, a controlled defense service performed for a foreign government entity using publicly available information may require a license.¹³¹ Likewise, although many marketing activities are exempt from ITAR licensing, certain marketing for significant military equipment is subject to licensing requirements.¹³² In addition, it is important to check the lists of restricted parties maintained by U.S. export controls regulatory agencies to ensure that you are not engaged in business with a designated entity.

It is also conceivable that when working for a foreign government customer—particularly in the Middle East—that you may face boycott requests. Indeed, simply a request to comply with local laws, in itself, could constitute a boycott request in countries identified by the U.S. Treasury Department on a quarterly basis as participating

in the Arab League boycott of Israel. (Boycott issues can also arise when dealing with entities from such countries when working in support of U.S. Government programs.)

Finally, while even in a contingency environment, U.S. Government contracting is generally a transparent process (though there will also be special risks dealing with local government authorities incident to such work), dealing with foreign government customers may present a new panoply of potential risks. Foreign government customers may have a less transparent procurement process, which may in turn raise corruption risks. Those risks will vary significantly based on the country in which the program—whether U.S. or foreign government-funded—is located as well as on the type of product to be delivered or service to be rendered. Thus, it is essential to assess country risk at the earliest stages of planning before becoming involved in a procurement abroad.

On a perhaps more mundane level, the U.S. Government is by statute required to pay its contractors promptly.¹³³ U.S. contractors should generally be aware that foreign government customers may not pay as quickly, that disputes with such customers may be resolved in unfamiliar fora pursuant to unfamiliar laws and regulations, and that the playing field may be tilted against them.

Know Your Partner

Teaming agreements are agreements entered into by two or more contractors to pursue a specific opportunity for purposes of joining qualifications and experience and combining bonding and resource capacity.¹³⁴ Generally, when entering into a teaming agreement, the due diligence necessary for a business partner that is a U.S. company and a larger player in the industry that it well known to you may be less demanding. Due diligence for lesser known companies, however, particularly foreign companies, can be more challenging and more critical to ensuring regulatory compliance.

■ U.S. Peer Group Companies

If you are a large U.S. Government contractor, many of the areas of compliance risk discussed

above will hopefully be familiar to you, though perhaps less so with regard to money laundering and boycott issues. To the extent that you are teaming with a similarly situated large company with a good reputation for business ethics, particularly one with which you have worked before, you may not need to engage in as much due diligence as when you are working with an unfamiliar entity, though some level of diligence is always prudent, particularly with respect to teams that may bid upon or perform significant programs in high-risk countries. Indeed, it is wise, at a very minimum, to ensure that you understand what policies and procedures and other internal controls a company has with respect to compliance with the FCPA and export controls in particular. Depending on the nature of the teaming relationship, e.g., prime contractor-subcontractor, special entity, or joint venture, it may be important to determine which company's set of policies and controls applies and what special compliance procedures may need to be implemented for the newly formed teaming entity.

Some of this can be done in a phased approach. When considering a company as a potential teaming partner, it is important to develop a general understanding of its compliance policies and procedures, as well as its overall reputation for business ethics. Sometimes this may necessitate requiring that the entity respond to a formal questionnaire or a formal interview. At the time you actually enter into a teaming agreement, it will be important to have the agreement itself state, in general, that the team will comply with various laws and regulations—most particularly, the FCPA and export controls—and to agree, in principle, how those issues will be dealt with by the team. Once the team actually wins work, it will be essential to put into force and implement team-specific policies and procedures.

■ Foreign Peer Group Companies

If you are teaming with a large foreign peer group company from a country that has long-established collaborative ties with the United States in the public procurement arena, such as Canada, the United Kingdom, Australia, or some other North Atlantic Treaty Organization allies, it is possible the company will have a compliance

culture similar to yours. It is also reasonably likely that the company will be accustomed to some of the extraterritorial aspects of compliance with U.S. law. Nonetheless, it is important to engage in diligence regarding such companies and to make expectations clear to them as to how and when U.S. law will, by necessity, apply. Large companies from these countries will often be familiar with U.S. anticorruption laws (and will themselves be subject to similar controls or local law constraints), though they may be less familiar with the U.S. export controls regime, which includes many concepts, such as the above-referenced “deemed export” and “reexport” restrictions, that are not commonly employed (or enforced) by other countries. It is important for the U.S. partner to understand with a greater degree of specificity how developed the large foreign partner’s compliance systems are and the extent to which policy enhancements should be implemented for the contract or project that the team seeks.

■ Smaller U.S. Companies

Some small companies are sophisticated in special compliance aspects of working abroad—others are not. To the extent that you are dealing with a smaller company, it is particularly important to understand what its experience has been as a Government contractor in the United States as well as abroad. Indeed, many smaller companies may have little or no understanding of export controls or the FCPA, let alone be aware of their intricacies, or of nuances regarding the interplay of foreign laws. Because a teaming partner has the ability to create potential legal liabilities or enforcement issues for the entire team, it makes sense to request specific information from a smaller company and to carefully discuss its compliance infrastructure before teaming with that company. Indeed, it most likely makes sense to specifically brief the company on compliance expectations and risks before finalizing a teaming arrangement.

■ Smaller Foreign Companies Or Non-Peer Group Entities

Teaming with smaller or non-peer group foreign companies, particularly those from countries outside of NATO or a handful of other close U.S. allies, frequently poses substantial risks.

Many—but by no means all—such companies likely have little or no understanding of compliance requirements of U.S. contracting. Beyond that, particularly in certain regions in the world, smaller or non-peer group companies may conceivably represent compliance risks due to lack of transparent ownership (including potential ties to foreign officials) or potential ties to individuals or entities involved in activities such as terrorism or money laundering (and may, therefore, be subject to certain elements of the OFAC sanctions regulations discussed above). It is often important to request a significant amount of information from such companies before entering into a teaming agreement. As with larger corporations, collecting information through a formal questionnaire, with additional followup as needed, makes sense, as does the implementation of special contractual provisions and internal controls applicable to performance.

■ Minority Partnership

There may sometimes be instances where, as a U.S. contractor, you act as a minority partner to a foreign contractor or where, as a condition of receiving a contract in another country, you must be a subcontractor and not a prime contractor or a minority owner of a joint entity. In such cases, it will nonetheless be important to ensure that the actions of the prime contractor, or of the overall entity, are not such that they create compliance risks. In other words, if you are a U.S. contractor doing work in tandem with a foreign partner that in its own right is unconstrained by U.S. sanctions regulations, for instance, you need to implement controls and governance structures for the mechanism such that your participation in the entity or the team does not, in itself, create sanctions risk. Likewise, your affiliation with a prime could result in FCPA risk or the risk of violating local anticorruption laws.

Know Your Third-Party Representatives

As numerous cases demonstrate, improper payments, or promises of improper payments, on the part of third parties such as sales agents can result in liability on the part of the company hiring such third parties.¹³⁵ Hiring third

parties can be a particularly risky undertaking in countries where corruption is perceived to be a problem. To manage such risks, appropriate precautions are in order. These include conducting due diligence regarding the third party's reputation or prior dealings and addressing and investigating any red flags that arise as a result of such efforts at due diligence. As in teaming, and perhaps more so, this process often involves extensive questionnaires and interviews of the third party, as well as inquiries to entities familiar with the third party. In addition, companies should include FCPA and anticorruption clauses in their contracts with third-party representatives and require various corruption-related certifications. Such FCPA and anticorruption clauses should give the company the right to terminate under certain circumstances as well as audit rights.

Companies should also conduct due diligence as to whether third parties appear on any of the sanctions or export control lists mentioned above. In addition, companies should take steps to ensure that third parties understand that their conduct cannot create compliance risks in other areas, such as with respect to export controls, sanctions, and antiboycott regulations. In this regard, agreements with third parties should address U.S. international regulatory compliance concerns above and beyond rules regarding corruption. Furthermore, companies may want to require compliance certifications addressing these areas. Finally, it is also common to require that third parties comply with certain policies and procedures, many of which implicate FCPA compliance considerations, such as those that relate to gifts and entertainment, travel and lodging, charitable contributions, and the like.

Know Your Subcontractor

■ U.S. Companies

U.S. companies, particularly peer group entities engaged regularly in foreign countries, generally are familiar with the FCPA and its prohibitions and thus may pose a somewhat lower risk as subcontractors. However, compliance policies

and cultures vary, and some companies may be more prone to risky business practices in terms of FCPA (or local corruption law) compliance. For this reason, companies may wish to apply the precautions listed above for third parties, including due diligence, contractual clauses, and certifications, to subcontractors that are U.S. companies as well. While it is difficult to conduct "formal" diligence in the context of U.S. Government subcontracting process, it is possible to elicit information in the request for proposals process that gives you a sense of a prospective contractor's ability to navigate international compliance concerns, and certainly it is possible to include specific clauses and controls in subcontracts as issued. Indeed, as the recent Baker Hughes settlement noted above (which did not occur in a U.S. Government contracting context) demonstrates, there is increasing concern by U.S. enforcement authorities about the conduct of subcontractors.¹³⁶

It is also important to be mindful of export controls and economic sanctions. Some large U.S. companies will be familiar with the need to comply with such regulations, others will not, and still yet others will wrongly assume that the mere fact that they are working pursuant to a U.S. Government procurement uniformly exempts them from the need to comply with export controls. When working with subcontractors, not only is it important to include relevant Federal Acquisition Regulation and Defense FAR Supplement clauses that address export controls and economic sanctions, but it may also be important to include your own clause stating that the subcontractor is aware of and will comply with export controls and delineating, as appropriate, which party in the course of contractual performance is responsible for the burden of obtaining licenses, if any. The clause should also make clear that the subcontractor is aware that export controls cover issues beyond the physical export of goods and also relate to the shipment of intangibles such as technical data or the sharing of technical data with foreign national employees in the United States or abroad. Subcontractors should be required to flow down these provisions to other subcontractors at any tier.

■ Foreign Companies

As subcontractors, foreign companies, particularly smaller entities, present many of the risks that foreign teaming partners represent. However, there may be an inadvertent tendency to be less concerned about the actions of foreign subcontractors than teaming subcontractor partners or first-tier U.S. subcontractors as they may be more removed day-to-day from your activities. However, if foreign subcontractors are unaware of U.S. compliance norms applicable to U.S. Government contracting abroad or of constraints that U.S. companies face when they work for foreign government customers, subcontractors can present similar risks. It is essential, therefore, that any subcontracts contain specific clauses regarding the compliance issues raised in this PAPER, and that such clauses be written in a clear and straightforward manner that foreign companies are able to understand and implement. Moreover, all foreign subcontractors, or even bidders, must be vetted against debarred

and restricted lists applicable to export controls and sanctions.

In many instances, U.S. contractors may also provide training materials to foreign subcontractors or even conduct training for them. Moreover, it may be necessary to implement specific policies and procedures applicable to those entities related to topics such as gifts and entertainment, travel and lodging, charitable contributions, and the like. U.S. contractors might also include specific information regarding compliance expectations in bid packages or mention such information in bidders' conferences. This provides encouragement for prospective subcontractors to view compliance as integral to successful contract performance, while at the same time acting as a warning or disincentive for those companies less apt to comply. Note also that there are DFARS provisions regarding subcontracting with entities owned or controlled by the government of a terrorist country, currently Cuba, Iran, North Korea, Sudan, and Syria, and in AID contracts, there may be additional country-based restrictions.¹³⁷

GUIDELINES

These *Guidelines* are intended to assist you in addressing diligence issues abroad. They are not, however, a substitute for professional representation in any specific situation.

1. Recognize that many statutes and regulations apply to work abroad. These include the FPCA, the MLCA, the OFAC sanctions, and the EAR and the ITAR, to name just a few. Each of these legal regimes is quite complex and the ramifications for potential violations are significant. Government expectations regarding compliance programs continues to evolve, and in certain areas, such as export controls and sanctions, the underlying regulations change with some frequency.

2. Assess country risk, even if working for the U.S. Government. Notwithstanding the fact that a U.S. Government program is involved, there may be important local law considerations, stringent export controls, or a local culture of corruption.

3. Be aware that entities with which you are dealing should also have an understanding of

the above regimes, as your partners' conduct has the potential to result in legal risk for you.

4. Carefully vet those with whom you work overseas. The diligence and vetting process will depend, in part, on the location in which you are working, the type of work you are performing, and the entity with which you propose to deal. While one size does not fit all and thus diligence can be calibrated and risk based, it cannot be ignored.

5. Pay particular care to relationships with teaming partners or with third parties such as sales agents. In each case, the risk that their conduct can be imputed to you may be significant.

6. Realize that diligence is the first, but not only, step in compliance, and that once you have agreed to work with partners, it is important to implement proper contractual compliance controls and risk mitigation strategies to help ensure proper project performance. Indeed, it is often important for these controls to be flown down through various contracting tiers.

★ REFERENCES ★

- 1/ Risen, "Contractor Deaths in Iraq Soar to Record," N.Y Times, May 19, 2007, at A1.
- 2/ See generally Goins, Fowler & Annus, "Regulating Contractors in War Zones: A Preemptive Strike on Problems in Government Contracts," Briefing Papers No. 07-3 (Feb. 2007); Irwin, "Special Compliance Considerations When Supporting the U.S. Government Abroad," Briefing Papers No. 04-7 (June 2004); McCullough & Edmonds, "Contractors in the Battlefield Revisited: The War in Iraq & Its Aftermath," Briefing Papers No. 04-6 (May 2004); Humphries & Irwin, "Teaming Agreements/Edition III," Briefing Papers No. 03-10 (Sept. 2003); McCullough & Edmonds, "Contractors in the Battlefield: Emerging Issues in Combat & Contingency Operations," Briefing Papers No. 02-7 (June 2002); Seyfarth Shaw LLP, *The Government Contract Compliance Handbook* ch. 19 (Thomson/West 4th ed. 2006).
- 3/ 15 U.S.C.A. §§ 78m, 78dd-1, 78dd-2, 78dd-3, 78ff. See generally Shaheen & Geren, "Foreign Corrupt Practices Act Enforcement Trends," Briefing Papers No. 05-8 (July 2005); Dyer, "Foreign Corrupt Practices Act," Briefing Papers No. 00-5 (Apr. 2000); Goddard, "Business Ethics in Government Contracting—Part I," Briefing Papers No. 03-6 (May 2003); Irwin, "Ethics in Government Procurement/Edition III," Briefing Papers No. 99-8 (July 1999).
- 4/ 15 U.S.C.A. §§ 78dd-1(a), 78dd-2(a), 78dd-3(a).
- 5/ See, e.g., *United States v. Kay*, 359 F.3d 738 (5th Cir. 2004) (payments allegedly made by principals of grain exporting corporation to Haitian government officials for purpose of reducing corporation's customs duties and taxes were potentially within FCPA's prohibition against payments to foreign officials to "obtain or retain" business).
- 6/ 15 U.S.C.A. §§ 78dd-1(f)(1), 78dd-2(h)(2), 78dd-3(f)(2).
- 7/ 15 U.S.C.A. § 78m(b)(2).
- 8/ 15 U.S.C.A. § 78m(b)(6).
- 9/ 15 U.S.C.A. §§ 78dd-1(g)(2), 78dd-2(i)(2).
- 10/ See, e.g., *United States v. Sapsizian* (S.D. Fla. 2006) (DOJ indictment charging a French citizen with eight counts of violating the FCPA antibribery prohibitions and conspiracy to violate the FCPA and the MLCA for allegedly conspiring to make over \$2.5 million in bribe payments to Costa Rican officials to obtain a telecommunications contract on behalf of Alcatel); DOJ Press Release No. 06-850, "Former Alcatel CIT Executive Is Indicted for Alleged Bribes to Costa Rican Officials To Obtain Mobile Telephone Contract" (Dec. 19, 2006), available at http://www.usdoj.gov/opa/pr/2006/December/06_crm_850.html.
- 11/ 15 U.S.C.A. §§ 78dd-2(g)(1)(A), (B), 78dd-3(e)(1)(A), (B), 78ff(c)(1)(A), (B).
- 12/ 15 U.S.C.A. §§ 78dd-2(g)(2)(B), 78dd-3(e)(2)(B), 78ff(c)(2)(B).
- 13/ 15 U.S.C.A. §§ 78dd-2(g)(2)(A), 78dd-3(e)(2)(A), 78ff(c)(2)(A); 18 U.S.C.A. § 3571(b).
- 14/ 18 U.S.C.A. § 3571(d).
- 15/ 15 U.S.C.A. §§ 78dd-2(g)(3), 78dd-3(e)(3), 78ff(c)(3).
- 16/ 15 U.S.C.A. § 78u(d)(3)(B); 18 U.S.C.A. § 3571(d).
- 17/ 15 U.S.C.A. § 78ff(a).
- 18/ FAR 9.407-2 (providing that contractors may be suspended upon adequate evidence of commission of fraud or criminal offense, including embezzlement, theft, and bribery). See generally West, Hatch, Brennan & VanDyke, "Suspension & Debarment," Briefing Papers No. 06-9 (Aug. 2006).
- 19/ 22 C.F.R. § 120.27(a)(6).
- 20/ International Anti-Bribery & Fair Competition Act of 1998, Pub. L. No. 105-366, 112 Stat. 3302 (1998).
- 21/ *United States v. Baker Hughes* (S.D. Tex. 2007) (Deferred Prosecution Agreement of Apr. 11, 2007); DOJ Press Release No. 07-296, "Baker Hughes Subsidiary Pleads Guilty to Bribing Kazakh Official and Agrees To Pay \$11 Million Criminal Fine as Part of Largest Combined Sanction Ever Imposed in FCPA Case" (Apr. 26, 2007), available at <http://www.usdoj.gov>.

- gov/opa/pr/2007/April/07_crm_296.html; SEC v. Baker Hughes Inc. & Fearnley, Case No. H-07-CV-1408 (S.D. Tex.) (Complaint filed April 26, 2007); SEC Litigation Release No. 20094 (Apr. 26, 2007), available at <http://www.sec.gov/litigation/litreleases/2007/lr20094.htm>; SEC Press Release No. 2007-77, "SEC Charges Baker Hughes With Foreign Bribery and With Violating 2001 Commission Cease-and-Desist Order" (Apr. 26, 2007), available at <http://www.sec.gov/news/press/2007/2007-77.htm>; United States v. Baker Hughes Servs. Int'l, Inc., Crim. Case No. H-07-129 (Information and Plea Agreement unsealed Apr. 26, 2007).
- 22/ United States v. Salam, (D.D.C. 2006) (Complaint); DOJ Press Release No. 07-068, "U.S. Civilian Translator Sentenced for Offering Bribes to Iraqi and U.S. Officials While Working in Adnon Palace in Baghdad" (Feb. 5, 2007), available at http://www.usdoj.gov/opa/pr/2007/February/07_crm_068.html.
- 23/ 18 U.S.C.A. §§ 1956, 1957.
- 24/ 18 U.S.C.A. § 1956(a)(1).
- 25/ 18 U.S.C.A. § 1956(a)(2).
- 26/ 18 U.S.C.A. § 1957.
- 27/ See 18 U.S.C.A. §§ 1956(c)(7), 1957(f)(3) (defining "specified unlawful activity"); see, e.g., United States v. Bloom (D.D.C. 2005) (Complaint); DOJ Press Release No. 07-089, "U.S. Contractor Sentenced in Case Involving Bribery, Fraud and Money Laundering Scheme in al-Hillah, Iraq" (Feb. 16, 2007) (U.S. Government contractor sentenced to 46 months in prison and ordered to forfeit \$3.6 million for conspiring to violate the U.S. domestic bribery statute and commit money laundering and wire fraud by making payments to a U.S. lieutenant colonel and the Coalition Provisional Authority comptroller in connection with construction contracts in Iraq), available at http://www.usdoj.gov/opa/pr/2007/February/07_crm_089.html.
- 28/ 18 U.S.C.A. § 1956(a).
- 29/ 18 U.S.C.A. § 1957(b); 18 U.S.C.A. § 3571.
- 30/ See 31 C.F.R. ch. V OFAC's website, <http://www.ustreas.gov/ofac>, also provides summaries of U.S. sanctions.
- 31/ 50 U.S.C.A. §§ 1701–1706.
- 32/ 50 U.S.C.A. app. §§ 1–44.
- 33/ See OFAC, Frequently Asked Questions and Answers, <http://www.ustreas.gov/offices/enforcement/ofac/faq/>.
- 34/ See *id.*
- 35/ See 31 C.F.R. pt. 515.
- 36/ See, e.g., 31 C.F.R. § 560.417 (Iran).
- 37/ 31 C.F.R. pt. 515.
- 38/ 31 C.F.R. pt. 560.
- 39/ 31 C.F.R. pt. 538. Sanctions against Sudan do not apply to specified areas of Southern Sudan where the Government of Sudan is not involved in the activity or transaction in question. Exec. Order No. 13,412, 71 Fed. Reg. 61,369 (Oct. 13, 2006).
- 40/ 31 C.F.R. pt. 537.
- 41/ See OFAC, Specially Designated Nationals and Blocked Persons List, available at <http://www.ustreas.gov/offices/enforcement/ofac/sdn/>.
- 42/ See <http://www.state.gov/s/ct/rls/fs/37191.htm>.
- 43/ See <http://www.un.org/sc/committees/1267/pdf/pdflist.pdf>.
- 44/ 31 C.F.R. § 501.801.
- 45/ Exec. Order No. 12,613, 52 Fed. Reg. 41,940 (Oct. 29, 1987); see also <http://www.treas.gov/offices/enforcement/ofac/programs/iran/iran.pdf>.
- 46/ Exec. Order No. 12,957, 60 Fed. Reg. 14615 (Mar. 15, 1995); Exec. Order No. 12,959, 60 Fed. Reg. 24,757 (May 6, 1995); Exec. Order No. 13,059, 62 Fed. Reg. 44,531 (Aug. 19, 1997); see 31 C.F.R. pt. 560.
- 47/ See H.R. 1400, 110 Cong. (2007) (proposed amendments to the 1996 Iran Sanctions Act and additional economic sanctions

- sponsored by Rep. Tom Lantos (D-Cal.) and Rep. Ileana Ros-Lehtinen (R-Fla.); S. 527, 110 Cong. (2007) (proposed amendments to the Iran, North Korea, and Syria Nonproliferation Act sponsored by Sen. Russell Feingold (D-Wis.)); S. 970, 110 Cong. (2007) (proposed sanctions against Iran sponsored by Sen. Gordon Smith (R-Ore.)).
- 48/ See S.C.Res. 1737, U.N.Doc.S/RES/1737 (Dec. 23, 2006), available at <http://www.un.org>.
- 49/ 31 C.F.R. pt. 538.
- 50/ Exec. Order No. 13,067, 62 Fed. Reg. 59,989 (Nov. 3, 1997).
- 51/ See 31 C.F.R. pt. 538; see also <http://www.treas.gov/offices/enforcement/ofac/programs/sudan/sudan.pdf>.
- 52/ Exec. Order No. 13,412, 71 Fed. Reg. 61,369 (Oct. 13, 2006).
- 53/ Pub. L. No. 108-175, 117 Stat. 2482 (Dec. 17, 2003); see Exec. Order No. 13,338, 69 Fed. Reg. 26,751 (May 11, 2004).
- 54/ See 31 C.F.R. pt. 542; 15 C.F.R. pt. 746 (regarding embargoes and special controls on Syria, as well as Cuba, Iraq, Iran, and Rwanda).
- 55/ 15 C.F.R. § 746.9, pt. 736, supp. 1, General Order No. 2.
- 56/ *Id.*
- 57/ See 15 C.F.R. § 746.3; see also 31 C.F.R. pt. 575.
- 58/ 31 C.F.R. pt. 500.
- 59/ 15 C.F.R. § 742.19.
- 60/ See Burmese Freedom & Democracy Act of 2003, Pub. L. No. 108-61, 117 Stat. 864 (2003); Exec. Order No. 13,310, 68 Fed. Reg. 44,853 (July 28, 2003); 31 C.F.R. pt. 537.
- 61/ See 31 C.F.R. pt. 545.
- 62/ See 10 C.F.R. pt. 810 (DOE); 10 C.F.R. pt. 110 (NRC).
- 63/ 22 C.F.R. pts. 120–130.
- 64/ 22 U.S.C.A. § 2778 et seq.
- 65/ See 22 C.F.R. pt. 120.
- 66/ See 22 C.F.R. pts. 122, 129.
- 67/ See 22 C.F.R. pt. 130.
- 68/ 22 C.F.R. §§ 120.14, 120.15, 120.16.
- 69/ 15 C.F.R. pts. 730–774.
- 70/ 50 U.S.C.A. app. §§ 2401–2420.
- 71/ 50 U.S.C.A. §§ 1701–1706.
- 72/ See 15 C.F.R. § 730.3.
- 73/ See 15 C.F.R. § 742.8 (Iran); 15 C.F.R. § 742.9 (Syria); 15 C.F.R. § 742.10 (Sudan); 15 C.F.R. pt. 746 (Cuba, Iraq, Iran, Rwanda, and Syria).
- 74/ 15 C.F.R. § 734.5.
- 75/ 22 C.F.R. pt. 121.
- 76/ 22 C.F.R. § 121.1(a).
- 77/ USML, Category XXI, 22 C.F.R. § 121.1.
- 78/ See 22 C.F.R. pts. 123, 125.
- 79/ 22 C.F.R. pt. 124.
- 80/ 22 C.F.R. § 126.4(a) (license exemption for temporary import or export of a defense article, technical data, or defense service by or for any agency of the U.S. Government for official use by such agency); 22 C.F.R. § 126.4(c) (license exemption for temporary import or temporary or permanent export of defense articles, technical data, or defense service for end use by a U.S. Government agency in a foreign country under certain circumstances); 22 C.F.R. § 125.4(b)(3) (license exemption for technical data in furtherance of a contract between the exporter and an agency of the U.S. Government, if the contract provides for the export of the data and such data do not disclose the details

- of design, development, production, or manufacture of any defense article); 22 C.F.R. § 125.4(b)(9) (license exemption for technical data sent by a U.S. corporation to a U.S. Government agency).
- 81/ See, e.g., 22 C.F.R. § 125.4(b)(1) (license exemption for export of technical data disclosed pursuant to an official written request or directive from the DOD); 22 C.F.R. § 125.4(b)(11) (license exemption for technical data for which the exporter has been granted an exemption pursuant to an arrangement with the DOD, DOE, or NASA).
- 82/ See 22 C.F.R. § 121.1.
- 83/ 22 C.F.R. § 126.1.
- 84/ 15 C.F.R. pt. 774, supp. 1.
- 85/ 15 C.F.R. § 772.1.
- 86/ 15 C.F.R. §§ 734.2(b), 734.3.
- 87/ 15 C.F.R. § 734.2(b)(2)(ii). See generally Burgett & Sturm, "Foreign Nationals in U.S. Technology Programs: Complying With Immigration, Export Control, Industrial Security & Other Requirements," Briefing Papers No. 00-3 (Feb. 2000).
- 88/ 15 C.F.R. §§ 734.2, 734.3.
- 89/ Id.
- 90/ See OFAC, Specially Designated Nationals and Blocked Persons List, available at <http://www.ustreas.gov/offices/enforcement/ofac/sdn/>.
- 91/ See <http://www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm>.
- 92/ See <http://www.bis.doc.gov/Licensing/ExportingBasics.htm>.
- 93/ 15 C.F.R. pt. 732, supps. 1, 2.
- 94/ 15 C.F.R. § 740.11.
- 95/ 15 C.F.R. pt. 747.
- 96/ Forexample, BIS fined ExxonMobil affiliates Mobil Services Company, Ltd., Mobil International Petroleum Corp., and Exxon Mobil Egypt (S.A.E.) \$49,500 for exporting laptops and servers to Sudan between 1999 and 2000. See <http://efoia.bis.doc.gov/ExportControlViolations/E892.pdf>.
- 97/ 15 C.F.R. pt. 738, supp. 1 (Commerce Country Chart).
- 98/ Id.
- 99/ 15 C.F.R. § 740.9.
- 100/ 15 C.F.R. pt. 747.
- 101/ 15 C.F.R. pt. 736, supp. 1, General Order No. 2.
- 102/ 72 Fed. Reg. 5614 (Feb. 7, 2007) (amending 22 C.F.R. § 126.1(a), (d) and adding § 126.1(k)).
- 103/ See http://www.bis.doc.gov/InternationalPrograms/Foreign_Language/Welcome_Arabic.htm.
- 104/ 50 U.S.C.A. § 1705; 18 U.S.C.A. § 3571; 15 C.F.R. §§ 764.3, 6.4(a)(4),(5).
- 105/ 50 U.S.C.A. § 1705.
- 106/ 22 C.F.R. §§ 127.3, 127.10; 22 U.S.C.A. § 2778(c), (e).
- 107/ 22 C.F.R. § 127.3; 22 U.S.C.A. § 2778(c).
- 108/ 15 C.F.R. § 764.3(a)(2).
- 109/ 22 C.F.R. §§ 127.7, 127.8; see also FAR subpt. 9.4. See generally West, Hatch, Brennan & VanDyke, "Suspension & Debarment," Briefing Papers No. 06-9 (Aug. 2006).
- 110/ See http://www.pmdtc.state.gov/consent_agreements.htm.
- 111/ See <http://www.bis.doc.gov/>; <http://www.pmdtc.state.gov/>.
- 112/ 50 U.S.C.A. app. § 2407.
- 113/ 15 C.F.R. pt. 760.
- 114/ 26 U.S.C.A. § 999.

- 115/ 15 C.F.R. § 760.2.
- 116/ 26 U.S.C.A. § 999(b)(3)(A).
- 117/ 26 U.S.C.A. § 999(b)(3)(B).
- 118/ 72 Fed. Reg. 15,934 (Apr. 3, 2007).
- 119/ 15 C.F.R. §§ 760.2, 760.5(b)(5).
- 120/ 15 C.F.R. § 760.1(b), (c).
- 121/ See 15 C.F.R. § 760.5(a).
- 122/ 26 U.S.C.A. § 999(a)(1); see <http://www.irs.gov/pub/irs-pdf/f5713sa.pdf>.
- 123/ 50 U.S.C.A. § 1705; 18 U.S.C.A. § 3571; 15 C.F.R. § 764.3.
- 124/ 50 U.S.C.A. § 1705; 18 U.S.C.A. § 3571; 15 C.F.R. § 764.3.
- 125/ 50 U.S.C.A. § 1705; 15 C.F.R. § 764.3.
- 126/ See <http://www.bis.doc.gov/antiboy-cottcompliance/CaseHistories/OACCCaseHistories4.html>.
- 127/ See 10 U.S.C.A. § 802(a)(10) (as amended by John Warner National Defense Authorization Act for Fiscal Year 2007, Pub. L. No. 109-364, § 552, 120 Stat. 2083, 2217 (2006)) (subjecting persons "serving with or accompanying an armed force in the field" to the Uniform Code of Military Justice).
- 128/ 22 U.S.C.A. § 2151 et seq.
- 129/ 48 C.F.R. § 752.225-70; see 22 C.F.R. pt. 228; see also 22 C.F.R. § 228.03 (identification of principal geographic code numbers); Irwin, "Special Compliance Considerations When Supporting the U.S. Government Abroad," Briefing Papers No. 04-7, at 6-7 (June 2004).
- 130/ See generally Seyfarth Shaw LLP, *The Government Contract Compliance Handbook* ch. 20 (Thomson/West 4th ed. 2006).
- 131/ 22 C.F.R. § 120.9(a)(1) (defining "defense service" as furnishing assistance to foreign persons in, among other things, the design, development, or manufacture of defense articles, furnishing technical data controlled under the ITAR to foreign persons, and military training of foreign units and forces).
- 132/ 22 C.F.R. § 126.8 (governing proposals to foreign persons relating to significant military equipment and stating that a presentation describing the equipment's performance characteristics, price, and probably availability for delivery would require prior notification or approval).
- 133/ 31 U.S.C.A. §§ 3901-3907; see 5 C.F.R. pt. 1315; FAR subpt. 32.9.
- 134/ See generally Humphries & Irwin, "Teaming Agreements/Edition III," Briefing Papers No. 03-10 (Sept. 2003).
- 135/ See, e.g., SEC Litigation Release No. 19107 (Mar. 1, 2005), available at <http://www.sec.gov/litigation/litreleases/lr19107.htm> (DOJ charged Titan Corporation for criminal violations of the antibribery provisions of the FCPA because it made payments to an agent in Benin who was a close advisor to the President of Benin and upon whom Titan had not conducted sufficient due diligence); DOJ Press Release No. 05-090, "Micrus Corporation Enters Into Agreement To Resolve Potential Foreign Corrupt Practices Act Liability" (Mar. 2, 2005); DOJ-Micrus Non-Prosecution Agreement (Mar. 2005), available at <http://www.usdoj.gov/dag/ctf/chargingdocs/micrusagreement.pdf> (Micrus Corp. was charged with violating the FCPA antibribery provisions because its agents, among others, made improper payments to doctors at state-run hospitals in France, Turkey, Spain, and Germany in exchange for contracts).
- 136/ *United States v. Baker Hughes* (S.D. Tex. 2007) (Deferred Prosecution Agreement of Apr. 11, 2007); DOJ Press Release No. 07-296, "Baker Hughes Subsidiary Pleads Guilty to Bribing Kazakh Official and Agrees To Pay \$11 Million Criminal Fine as Part of Largest Combined Sanction Ever Imposed in FCPA Case" (Apr. 26, 2007), available at http://www.usdoj.gov/opa/pr/2007/April/07_crm_296.html; *SEC v. Baker Hughes Inc. & Fearnley, Case No. H-07-CV-1408* (S.D. Tex.) (Complaint filed April 26, 2007); SEC Litigation Release No. 20094 (Apr. 26, 2007), available at <http://www.sec.gov/litigation/litreleases/2007/lr20094.htm>; SEC Press Release No. 2007-77, "SEC Charges Baker Hughes With Foreign Bribery and With Violating 2001 Commission Cease-and-Desist Order" (Apr. 26, 2007), available at <http://www.sec.gov/news/press/2007/2007-77.htm>; *United States v. Baker Hughes Servs. Int'l, Inc., Crim. Case No. H-07-129* (Information and Plea Agreement unsealed Apr. 26, 2007).
- 137/ DFARS 252.209-7004; see also FAR 52.225-13.

THOMSON
——™
WEST