

CORPORATE COMPLIANCE INSTITUTE

INTERNATIONAL COMPLIANCE ISSUES

Giovanna M. Cinelli
Partner
Patton Boggs, LLP

INTERNATIONAL COMPLIANCE ISSUES

Giovanna M. Cinelli
Partner
Patton Boggs LLP
McLean, Virginia

Globalization - the buzzword of the 21st Century. Between outsourcing, offshore procurement, international joint ventures, teaming arrangements, and related international cooperative efforts, all companies, of whatever size, touch upon some aspect of the new "globalized world." From a legal perspective, this change represents a foray into a quagmire of new requirements. "Conflicts" of law - in the broadest sense - take on a new meaning. While the United States has a myriad of laws that apply to both public and private companies, the U.S. is not alone. Each country has its own corporate, tax, intellectual property, national security, defense, environmental, bribery and similar other mandates. In addition, several countries preclude corporate entities subject to their jurisdiction from complying with the "extraterritorially imposed requirements" of other sovereign nations. How does one navigate these differing and sometimes competing or conflicting obligations? Equally important, how does one determine what these obligations entail and subsequently incorporate them into a coherent compliance program?

This presentation is divided into two sections. Part One identifies some of the key laws that apply to "globalized" companies. Part Two outlines factors to consider when establishing international compliance programs, including modifications to the basic elements of most programs to address specific issues related to "globalized activity."

I. APPLICABLE LAWS AND REGULATIONS

The terms, "globalization," the "global environment," and "global operations," are all used frequently in the lexicon of international activity. The Defense Sciences Board recently issued a study defining "globalization" and noting its inevitability. *Final Report of the Defense Science Board Task Force on Globalization and Security*, Office of the Under Secretary of Defense for Acquisition and Technology, December 1999. "Globalization" means "the integration of the political, economic and cultural activities of geographically and/or nationally separated peoples." *Id.* at i, 5. Whether referencing cross-border operations established in several countries or employment of an international workforce, companies today need to establish ground rules for approaching those activities which extend beyond U.S. borders and U.S. laws. This is critical in terms of dealing with U.S. laws designed to reach activity of U.S. companies, wherever conducted.

Within the confines of global operations or international business, companies need to be aware of multijurisdictional statutes and regulations that address, at a

minimum, exports, imports, graft, corruption, payments to consultants and the flow of people across borders. From the U.S. perspective, this means that compliance programs need to include, but not be limited to, the following laws and regulations:

1. U.S. Export Laws: Export Administration Act of 1979, 50 U.S.C. App. §§ 2401 to 2420 (as amended) (“EAA”); Arms Export Control Act, 22 U.S.C. §§ 2778 *et seq.* (“AECA”); Trading with the Enemy Act, 50 U.S.C. App. §§ 1 to 44 (1998) (“TWEA”); International Emergency Economic Powers Act, 50 U.S.C. App. §§ 1701 *et seq.* (“IEEPA”); the Export Administration Regulations, 15 C.F.R. part 730, *et seq.* (“EAR”); the International Traffic in Arms Regulations, 22 C.F.R. part 120, *et seq.* (“ITAR”); and the Foreign Assets Control Regulations, 31 C.F.R. part 500, *et seq.* (“OFACR”);
2. Graft and Corruption Laws: Foreign Corrupt Practices Act, 15 U.S.C. §§ 78m, 78o, 78dd-1 to 78dd-3, 78ff (“FCPA”);
3. Antiterrorism Laws: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, P.L. 107-56, 115 Stat. II 272 (2001) (the “U.S. Patriot Act”) (incorporated into over 150 statutory citations) see Attachment 1; and
4. U.S. Immigration Laws: 8 U.S.C. §§ 1101, 1551, *et seq.*

Furthermore, the events of September 11, 2001, have produced an “anti-terrorism” overlay to existing international activity by inserting additional screening, reporting, tracking and licensing requirements to previously fairly unregulated activities. This overlay, coupled with the reach of U.S. laws, has created a tension within the international community that makes compliance with U.S. laws and other nation’s requirements more difficult.

Each of the laws noted above imposes obligations on business and are discussed below.

A. United States Export Laws

1. EAA and EAR
 - a. Controls the export of dual-use goods and technology, including materials, production equipment and software itemized on the Commerce Control List;
 - b. Controls exports through a licensing regime that requires approval from the Department of Commerce prior to shipping any item referenced in (a), above;

- c. Is administered by the Department of Commerce in consultation with a number of U.S. Government agencies, depending upon the type of export;
- d. Mandates that extensive records be kept and reports be provided for antiboycott requests;
- e. Applies to exports and reexports of U.S. items referenced in (a), above, depending upon the degree of U.S. content in each item or technology (10%/25% *de minimis* standards); and
- f. Applies to foreign persons, as well as U.S. persons, whether in the United States or abroad.

2. AECA and ITAR

- a. Controls the export and temporary import of defense articles, technical data and defense services itemized on the U.S. Munitions List;
- b. Requires export licenses or temporary import licenses be obtained from the Department of State prior to shipping any item, technical data, software or related article or providing any defense service as defined in the ITAR;
- c. Is administered by the Department of State in consultation primarily with the Department of Defense;
- d. Imposes extensive recordkeeping and reporting requirements;
- e. Requires registration with the Directorate of Defense Trade Controls as a prerequisite to obtaining any export authorizations from State;
- f. Applies to exports, temporary imports and reexports of any item, technical data or defense service enumerated on the U.S. Munitions List;
- g. Applies to foreign persons, as well as U.S. persons, whether in the United States or abroad; and
- h. Allows U.S. persons to obtain any authorization permitted under the regulations. Allows foreign persons, in select circumstances, to obtain reexport authorizations.

3. Increased Enforcement

- a. The export laws have been vigorously enforced, in both a civil and criminal context, over the last seven years.

- b. The Department of Commerce aggressively enforces the various regulations, whether covering the unlicensed exports of goods and technology or failures to file antiboycott reports with the Bureau of Industry and Security. Cases have also been referred to the Justice Department for prosecution. Fines range from \$5,000 to \$18 million. Companies that have been fined include IBM, Alcoa, Allergan, L'Oréal and Halliburton.
- c. The Department of State has also aggressively enforced the export laws, primarily within the last five years. Several defense contractors – notably The Boeing Company, Lockheed Martin Corporation, Raytheon, Hughes Electronics Corporation, Loral Space Systems and the Loral Corporation, EDO Corporation, Agilent and Motorola – have paid fines ranging from \$80,000 to \$32 million. In addition, fines have been assessed against individuals in the \$500,000 range, most recently against Dr. Wah Lim, a senior vice president employed by both Loral and Hughes.
- d. Enforcement at both State and Commerce extends now to areas previously not viewed as export-related: unauthorized exports during the course of litigations; a failure to conduct adequate due diligence in the export arena; and unauthorized exports occurring during M&A activity. Companies have faced either fines or other penalties, primarily from the Department of State, for these alleged violations.

B. Foreign Corrupt Practices Act

- 1. Criminal and civil statute which controls international activity related to payments made to certain individuals;
 - a. Is administered by the Department of Justice;
 - b. Prohibits the payment of monies to certain individuals holding government or political positions;
 - c. Requires that specific records be kept and reports be made of payments to such individuals;
- 2. Was initially in place only in the United States;
- 3. Governs the activities of publicly traded companies or issuers of stock;
- 4. Controls similar to the FCPA have now been adopted by a number of countries through the OECD "Convention on Combating Bribery of Foreign Public Officials in International Business Transactions."
 - a. As of December 17, 2003, 35 countries have ratified the Convention and agreed to be bound by its precepts. Those countries include: Iceland,

Japan, Germany, Hungary, the U.S., Finland, the United Kingdom, Canada, Norway, Bulgaria, South Korea, Greece, Austria, Mexico, Sweden, Belgium, the Slovak Republic, Australia, Spain, the Czech Republic, Switzerland, Turkey, France, Brazil, Denmark, Poland, Portugal, Italy, the Netherlands, Argentina, Luxembourg, Chile, New Zealand, Slovenia and Ireland.

- b. Each country has implemented laws and regulations governing the payment of monies to political or governmental officials. See Attachment 2. Increased penalties, forfeiture, the criminalization of bribery and expansion of the various laws' applications are included in the countries' approaches.
5. The United States, in ratifying this Convention, has modified the FCPA, to cover any requirements of this international agreement not already included in the FCPA.
6. The FCPA and related international laws remain especially sensitive areas since consultants and representatives are widely used to obtain business for companies. The effectiveness of consultants or representatives partially stems from the individual's contacts with government or political personnel, personal relationships with government personnel, or payments made to these individuals to influence various procurement decisions.
7. Enforcement exists, but is not as aggressive as in the export arena. However, political sensitivities and corporate reputations counsel that lack of enforcement not be considered a dispositive factor in triaging compliance with these laws.

C. The U.S. Patriot Act

1. The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001," also known as the "Patriot Act," was passed in response to the tragic events of September 11, 2001. This legislation provides the U.S. Executive Branch expanded investigatory and monitoring powers, additional controls over people's access to the United States, limitations on due process in certain circumstances and restrictions on certain information subject to U.S. jurisdiction. This legislation authorized:
 - a. registration requirements for certain foreign people in the United States on visas;
 - b. limitations on judicial review for detention of suspected "enemies of the State" or suspected terrorists;

- c. new regulations affecting information sharing with the U.S. Government by insured depository institutions;
 - d. new restrictions on monetary transfers to address potential money laundering activities;
 - e. expanded screening requirements for entities that may finance or otherwise support terrorist activities;
 - f. extraterritorial application of the law to terrorism which transcends national boundaries;
 - g. additional authorities, which may be found in Attachment 1.
2. Although considered tragic and decried by the international community, legislative reaction to the events of September 11th within that community have been slow or nonexistent. Unlike the United States, which immediately implemented rigors to increase accountability of individuals within the U.S. and of companies or monetary institutions transacting internationally, most countries have not changed their laws. Assuming that Congress renews or enhances the legislation's current authorities and courts do not find the statute, in whole or in part, unconstitutional, this legislation directly affects a number of activities conducted by U.S. companies, whether in the U.S. abroad. These activities include the hiring and training of foreign individuals, international monetary transfers and the level of due diligence required to confirm the end-users and end-uses of items within international transactions. Recordkeeping and reporting requirements for international institutions, including universities, academic institutions and other research organizations, also increased.

D. Immigration Statutes

United States laws have always controlled a foreign person's entrance into the United States, whether for business, work or pleasure. *See, e.g.,* 8 U.S. C. §§ 1101, 1151 *et seq.* In general, the United States requires visitors to the U.S. to physically enter the country through specific locations, using a process that allows the Government to account for the individuals' presence in the U.S. Visas may be required to visit the U.S., but are certainly mandatory for study or work in the U.S. Although the Departments of Justice and Homeland Security now administer the visa and citizenship process under the Patriot Act and other immigration legislation, other agencies also participate in the process. For example, admission of a foreign national into the United States to work for a U.S. company may require the issuance of an export license for the prospective employee to have access to goods, technology, or data resident within the U.S. company's facilities. Export licenses, depending upon the type of good or technology, may be issued by either the Department of State or the Department of Commerce through bureaus or offices that have no direct relationship to agencies that administer the immigration laws. State periodically deals with visa and related policy

issues involving access to the United States or with diplomatic and dignitary issues. The Commerce Department, however, rarely does, with the exception of exchange programs it may sponsor for visiting dignitaries. A number of agencies, therefore, could affect the compliance programs of global companies moving international employees across facilities.

The degree of immigration enforcement varies, depending upon whether the Government is dealing with illegal immigration across U.S. borders, universities' inability to account for foreign students in the U.S. on student visas, or the abuse of intracorporate visa transfer programs. See, e.g., *Homeland Security: Overstay Tracking is a Key Component of a Layered Defense*, Testimony before the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives, GAO-04-170T, (General Accounting Office, October 16, 2003); *Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process*, Report to Congressional Committees, GAO-03-1084R (General Accounting Office, August 18, 2003); *The Immigration and Naturalization Service's Contacts with Two September 11 Terrorists: A Review of the INS's Admissions of Mohamed Atta and Marwan Alshehhi, its Processing of their Change Status Applications and its Efforts to Track Foreign Students in the United States*, Office of the Inspector General, Department of Justice, May 20, 2002.

The international community, however, does not address immigration issues in the same manner as the United States. Several countries permit citizens to hold multiple citizenships and passports. See, e.g., Canada and members of the European Union. And some countries or organizations, notably, the European Union, strive for an elimination of "borders" within member states, actively supporting the concept of "the right to work" in any member state, without the need for additional authorizations. Given the differences in accountability between the U.S. and the international community, a number of conflicts can arise in the hiring policies, privacy policies or work processes of global companies.

II. FACTORS TO CONSIDER WHEN IMPLEMENTING A COMPLIANCE PROGRAM FOR GLOBAL OPERATIONS

In general, a compliance program is designed to manage a company's compliance with laws and regulations. Any program should highlight the relevant legal requirements, communicate directly with employees concerning their obligations under the laws, and manage risk. All compliance programs begin from the top: Board of Director and senior management support is essential to the success of any program, no matter how well written. The support, however, needs to be more than just words - since policies are easy to write. It needs to be demonstrated through management action, notably the allocation of sufficient financial and human resources to meet the obligations comfortably.

The need for management support and the allocation of resources becomes increasingly complex when dealing in an international environment. Apart from

conflicting legal obligations - e.g., the data privacy requirements within the European Union versus the interpretation of privacy limitations in the United States - the allocation of sufficient resources which affect an international entity's bottom line becomes a sensitive issue. Whose management determines what applies, to whom, under what circumstances and for what cost are frequently asked questions, especially when dealing with the foreign subsidiaries of U.S. companies or even the U.S. subsidiaries of foreign parents. What then needs to be included in any management program and how should it be structured?

A. Basic Elements of a Global Compliance Program

1. Compliance Programs all require:

- a. policies from management mandating compliance;
- b. the identification of human resources within the corporate structure to support the compliance obligations;
- c. the establishment of procedures that govern licensing, registration, reporting or compliance with U.S. Government standards;
- d. training in the relevant legal obligations for personnel in general, as well as those specifically tasked to complete certain compliance responsibilities;
- e. auditing processes and a schedule for audits, both internal and independent, to ensure that the compliance program addresses the needs of the business, as well as to monitor the effectiveness of the program;
- f. a clearly stated enforcement process that notifies employees of the consequences of noncompliance;
- g. a mechanism for dealing with noncompliance, whether willful or inadvertent;
- h. a mandatory recordkeeping process that specifically identifies those records that need to be maintained for what period of time; and
- i. the establishment of a mechanism to monitor and update a company's legal obligations.

2. The effectiveness of a basic program generally relies on three elements:

- a. Simplicity
 - i. clear language in any written documentation;

- ii. easily understood processes, usually linear; and
 - iii. if possible, flow-charted.
- b. Communication
 - i. broad and frequent;
 - ii. in writing and verbal; and
 - iii. provided by various layers of management, beginning with the most senior individuals.
- c. Risk management
 - i. a keen understanding of the monetary limits to any compliance program;
 - ii. a realistic assessment of the consequences for failing to comply, to the fullest, with legal obligations;
 - iii. an analysis of the Sarbanes-Oxley requirements impacting any international compliance program; and
 - iv. a list of the laws which must be complied with or should be complied with, based on reasonable business judgment.

B. Modifications or Additions to a Basic Program

Given the basic elements a company should include in its compliance program, what particular issues need to be addressed for global companies that do not necessarily appear for domestic companies? Some modifications or issues involve process issues. Others relate to substantive areas of laws requiring specific compliance structures. The following list provides a number of process and substantive issues that should be addressed.

1. Translations: Global companies should be prepared to translate all their policies, legal requirements, training and procedures into all foreign languages covering their employee base. In addition, responsible personnel within the company should be fluent in a number of languages to be prepared to answer questions for employees or to discuss legal interpretations of compliance requirements.
2. Visa Monitoring Program: Global companies should include an increased and robust visa monitoring system to ensure that business is not adversely affected by lapsed visas prohibiting members of the international workforce from maintaining employment. In addition, companies should include monitoring with similar controls of any students on F-1 practical training visas working for companies. Representatives

from Human Resources and Legal should work closely together to ensure compliance in this area.

3. Export Licensing Program: Global companies should include a broad-based, sophisticated export licensing, classification and license administration program designed to streamline business operations around licensing requirements. This program should involve representatives from the Legal, Human Resource, Security, Research & Development and Technical functions within a company. Each of these functions plays a vital role in satisfying export obligations.
4. Recordkeeping Policies that Address Broad Issues: Recordkeeping requirements under U.S. laws vary depending upon the reason for control. For example, most companies maintain policies that mandate destruction of e-mail records after 90 days. This policy exists, ostensibly to prevent the crippling of global companies' intracompany networks and because laws do not exist specifically controlling the retention of e-mails for all reasons. This policy, however, fails to meet the requirements of the export laws, for example. The export laws impose a five-year recordkeeping requirement on any item (including software, technical information or technical data) subject to their control. Therefore, an engineer in the U.S. who e-mails specifications to a fellow employee in Austria, needs to keep the e-mail and the specification for a five-year period from date of transmission. If a company automatically destroys all e-mails after 90 days, the company *de facto* fails to meet this requirement and has violated the EAR or the ITAR. The same holds true for international obligations.
5. Data Privacy Requirements: Global companies should institute a clear policy on the type of information that may be kept on employees and shared with others, whether within the company and all its operations or with the government of any sovereign nation. The policies and proposed regulations of the European Union in particular raise serious concerns related to the sharing of individuals' personal information.
6. Confidentiality Requirements: Any company with global operations needs to contend with the confidentiality of technical information transferred among employees, temporary help, consultants or representatives. The sharing of this information implicates the export laws, as well as a number of intellectual property laws. Failure to protect technical information and enforce the terms of confidentiality agreements with employees jeopardizes a company's intellectual property position, as well as its export compliance posture with the U.S. Government. Confidentiality agreements and a process to renew them should be instituted as part of ongoing employee training, as well as included in all agreements with outside resources. Confidentiality agreements and related policies should

be drafted in English and the native language of all countries where the company maintains operations.

7. Outsourcing Policy: Recent press articles note an increasing trend for companies to outsource functions – everything from contracts to technical reviews to legal advice to document preparation. The reasons cited predominantly focus on decreased costs for labor, as well as limitations on the benefits that need to be provided to outsourced resources. Understanding the limits of outsourcing and the risks associated with potential violations of laws affected by outsourcing is critical.

Although not designed to eliminate or address all problems arising within a global compliance program, the issues and highlights noted above represent an initial approach to meeting international compliance obligations.