FOLEY & LARDNER LLP

Coping with U.S. Regulation of International Conduct: Compliance Strategies for U.S. Export Controls and Sanctions Regulations

Gregory Husisian
Foley & Lardner LLP
3000 K Street, NW, Suite 600
Washington, DC 20037-5143
202.945.6149
ghusisian@foley.com

November 2009

Coping with U.S. Regulation of International Conduct: Compliance Strategies for U.S. Export Controls and Sanctions Regulations

In recent years, the U.S. Government has become increasingly aggressive in enforcing U.S. laws designed to regulate the conduct of U.S. citizens and companies operating abroad. As a result, multinational firms face multiplying compliance concerns, especially with regard to the Foreign Corrupt Practices Act, export control and sanction regulations, the anti-boycott law, and anti-money laundering requirements. In the second of three articles, the author presents compliance strategies for corporations attempting to manage the risks posed by U.S. export controls and sanctions regulations.

GREGORY HUSISIAN
FOLEY & LARDNER LLP

INTRODUCTION

Export control and sanction requirements have been around for years, but are taking on increasing prominence. Long thought of as a risk only to companies that shipped to rogue states or engaged in high-risk financial transactions, these laws today are of increasing concern to all financial institutions and exporters subject to U.S. jurisdiction. In fact, the U.S. Government has announced that sanctions and export-control enforcement is a top priority. On October 11, 2007, the DOJ announced a comprehensive National Counter-Proliferation Initiative, which will involve the DOJ working with special agents from the BIS Office of Export Enforcement, Immigration and Customs Enforcement (ICE), Customs and Border Protection, and the FBI to target export control and sanction violations.[1]

Export control and sanction requirements are principally administered by three U.S. Government agencies:

- ***DDTC.*** The State Department's Directorate of Defense Trade Controls ("DDTC") administers the International Traffic in Arms Regulations ("ITAR"),[2] which cover the export and brokerage of defense-related

[1] Press Release, Department of Justice, *Justice Department and Partner Agencies Launch National Counter-Proliferation Initiative* (Oct. 11, 2007), *available at* http://www.usdoj.gov/opa/pr/2007/October/07_nsd_806.html.

[2] 22 C.F.R. Parts 120–130.

articles, services, and technology.[3] The ITAR cover items specifically designed or modified for military use, but in certain cases items with non-military uses, such as commercial communications satellites, have been brought within the rubric of coverage. Companies that produce defense articles or provide defense services are subject to a variety of requirements, including registration, licensing, and sales restrictions.

- ***BIS.*** The Commerce Department's Bureau of Industry and Security ("BIS") administers the Export Administration Regulations ("EAR"),[4] which pertain to the export of goods and technologies not covered by the ITAR. These dual-use items are subject to varying controls, depending upon the product or technology, destination, and end user. Dual-use items are suitable for either military or non-military use and are not designed or modified for military use (which would subject them to ITAR purview).
- ***OFAC.*** The Treasury Department's Office of Foreign Assets Control ("OFAC") administers most economic sanctions regulations, which prohibit or restrict transactions and investments in countries with adverse foreign policies or persons taking actions inimical to U.S. interests (*e.g.*, terrorists or persons aiding sanctioned governments).[5] Depending upon the particular restriction at issue, OFAC regulations can restrict exports and imports to blocked entities or countries, the provision or purchase of services, financial transactions with blocked countries or entities, and restrictions on travel, among other restrictions.

ESTABLISHING AND IMPLEMENTING AN EFFECTIVE COMPLIANCE PROGRAM

The requirements of export controls and sanctions laws and regulations are nuanced and the requirements, in many cases, unforgiving. Difficult issues of interpretation abound, and even experienced companies find compliance with these complicated regulations to be daunting. Nonetheless, risk management is possible.

The basic compliance tasks for exports and financial transactions are well known. The goal is that there be no exports of goods, services, or technology, or completion of a financial transaction, unless it has been established that:

- there is the general authority to make the export to the intended recipient in the intended country of destination or to engage in the transaction;

[3] *See* 22 C.F.R. Parts 120-130.

[4] *See* 15 C.F.R. Parts 730-774.

[5] *See* 31 C.F.R. Parts 500-598.

- the export or transaction is authorized by U.S. Government regulations, whether by general authority, specific license applicability, or exemption;
- all required documentation is prepared; and
- all relevant records are kept for the required period.

The most important risk-management tool to accomplish these goals is a good compliance program. Too many companies, however, do not take compliance seriously, instead thinking of compliance as a cost and business burden.

But in today's business environment, the better mindset is to view compliance as a means of ensuring the proper discharge of basic corporate responsibilities by moderating and controlling risk. A good compliance program does more than just deter violations—it also helps to detect the violation once it has occurred, provides an internal mechanism to report it, prevents the violation from growing into a pattern, allows the company to conduct an internal review to determine what happened, and helps the company put in place appropriate remedial measures. It serves education, deterrent, and discovery functions. In the event that the problem reaches the government, it also helps convince the government that, as a good corporate citizen, a civil rather than criminal approach is needed and that any fine assessed should be lower because the existence of a pre-existing compliance program is an important mitigating factor.[6] By serving all these functions, a compliance program is a key investment in risk mitigation, thereby helping the firm carry out its corporate objectives in a prudent and managed fashion.[7]

There also is a good business case for strong compliance. The due diligence required under a proper program often can ferret out the kind of unreliable customers and business partners who tend to cause corporate troubles. But even absent such benefits, only the most foolhardy exporter or financial institution proceeds without a good compliance program in place.

Creating a Culture of Compliance

According to the U.S. Sentencing Guidelines Manual, an effective compliance program requires an organization to "exercise due diligence to prevent and detect [wrongful] conduct" and "otherwise promote an organizational culture that

[6] *See Federal Sentencing Guidelines* § 8C2.5(f).

[7] In other contexts, failure to have a compliance program has been viewed as being sufficient to support a claim of recklessness. In *United States v. Merck-Medco*, the government contended that the failure of the defendant to put in place an adequate compliance program, in and of itself, indicated that the company had acted with reckless disregard. The Court held as a matter of law that the failure to have such a compliance program could be used in this fashion. *See* 336 F. Supp. 2d 430 (E.D. Pa. 2004). Another sobering case is *In re Caremark Int'l Inc. Derivative Litigation*, where the Delaware Court of Chancery held that corporate directors have a fiduciary duty to assure that a corporation has "information and reporting systems" to prevent wrongdoing and that failure to have them could be the basis of derivative suits alleging violations of the anti-kickback statute and the False Claims Act. *See* 698 A.2d 959 (Del. Ch. 1996).

encourages ethical conduct and a commitment to compliance with the law."[8] Compliance seldom accomplishes these aims unless there is a top-down initiative to underscore the importance of the program. This means that there should be buy in for the program from the Board of Directors, top management, and other key internal actors. Compliance should not be seen as a purely legal issue; it should be seen as one of importance to the proper operation of the company. These goals are effectuated by close attention to the following:

- ***Giving Compliance Internal Status.*** Creating a culture of compliance starts with education. Companies should make compliance a funding priority so that there are sufficient resources to run the program. The person in charge of compliance should have the authority to stop transactions and shipments, without question, until red flags are satisfied. Compliance should also be run independent of sales or business generation to prevent pressure to overlook red flags. Most importantly, companies should have a well established chain of communication to ensure that important compliance-related concerns get the ear of top management, whether through the General Counsel's office or otherwise.
- ***Tailoring Compliance***. In times past, it was common to find compliance programs that were similar from company to company. The better practice, however, is to tailor the program. Companies should review all facets of the business, including the goods sold, the technology exported, and the technology used in production. They should review typical sales patterns—does the company sell products in controlled industries, or to controlled environments or people? Does it rely on restricted technology? Does it primarily sell to end users, resellers, or to companies that incorporate U.S. technology into other products? Company-specific factors dictate the best compliance for each company.
- ***Moving Beyond Shipping.*** Traditionally, exporters cordoned off compliance to a corner of the company, bringing compliance into play only when it came time to ship or when a new account was opened. A better mindset, however, is to create a compliance mentality by training everyone on at least the basics of export-control and sanctions requirements using an "A/B/C" training mentality—basic, perhaps online only, C-level training for most employees, more detailed training for people involved in sales or high-risk financial areas, and intensive, A-level training for people on the front lines of compliance. Common red flags (like those listed in the Appendix to this chapter) should be known throughout the corporation, so that every employee can help prevent costly violations.

[8] U.S. 2008 Federal Sentencing Guidelines Manual, § 8B2.1 (Nov. 2006).

- ***Involving Third Parties.*** Many companies put procedures in place for the vetting of third-party relationships, including through the performance of systematic due diligence. The procedures for vetting these relationships should rely on people who are not directly associated with the completion of the transaction to ensure high levels of objectivity.

Companies, too, should consider how they will follow up on compliance initiatives. The involvement of senior management does not end once the program is rolled out. Many companies incorporate compliance concepts into employee performance reviews, so that some portion of the employees performance evaluation is based on adherence to compliance standards. The company also should have in place methods for employees to report compliance concerns that are independent of normal business channels, so employees know they can share concerns without fear of retribution.

Taking Advantage of Technology

Technological innovations have penetrated the compliance realm. The value of the tools cannot be disputed, since they automate a lot of time-intensive screening. There is, however, a fine line between responsible implementation and over-reliance on automated tools.

- ***Screening Software.*** In prior incarnations, the heart of compliance was a matrix that listed every product sold and its export status. This was cumbersome and thankfully is automated by widely available export screening software and websites, such as Export Control Resource's ExportWeb. These software packages also are invaluable for the tedious task of checking lists of SDNs.
- ***Automated Recordkeeping.*** Exporting has always required a lot of tracking responsibilities. Today, however, requirements to transmit information about exports electronically via the Automated Export System ("AES") make keeping good records critical, because AES data is shared among numerous U.S. agencies. BIS, DDTC, and OFAC can, and do, request supporting documentation for certain transactions,[9] as does OFAC for financial transactions.
- ***Linking Systems.*** Many larger freight forwarders and shippers routinely screen shipments. It is becoming increasingly common for companies to integrate their procedures for screening with those of their shipping companies, especially now that there is an increasing number of cases targeting freight forwarders and other shippers.[10]

[9] As indicated in the ITAR, the "AES shall serve as the primary system for collection of export data for the Department of State," although "requests for special reporting may be made by DDTC on a case-by-case basis." ITAR § 120.30.

[10] *See, e.g., Kabba & Amir Investments, Inc. d.b.a. International Freight Forwarders*, Dkt. No. 05-BIS-08 (Apr. 30, 2008) (delivery and insurance for articles to Cuba); *United States v. DSV Samson Transport*, Crim. Action No. 03-cr-00296 (D.D.C. 2003).

Moving Beyond a ‘‘Goods’’ Mentality

Export control compliance programs traditionally focused on goods because no export meant no violation. But this attitude, while never particularly accurate, is becoming less and less relevant. Forbidden transfers of technical data can occur whenever there are communications with customers, vendors, joint venture partners, foreign affiliates, visitors, or foreign employees. Emails, faxes, database access, and conversations are all possible violations of restrictions on the export of information. All of these potential danger points have to be taken into account through careful consideration of the following key points:

Technology. Export compliance for technology requires a different mindset, with the focus as much on the process of creation and the use of the product as the good itself. For example, where software is at issue, the focus is not on the physical medium but rather such issues as the method of export (which could be over the internet and thus not involve any good in traditional form) and the potential uses of the software (which might be incorporated into a controlled product by the purchaser). Goods with encryption raise a host of related issues.

Non-Traditional Exports. Technology also brings into play non-traditional means of export. Such issues as whether there is a “deemed export” (*i.e.*, communication of controlled information to a non-U.S. national, whether by oral discussion, visual inspection, or otherwise), export by access to a company’s information systems, issues relating to the employment of non-U.S. nationals, or even whether the mere exposure of a foreigner to a “data-rich environment” are all potential violations that are amplified where highly technological goods and services are at issue. A good compliance program requires a review of all business operating processes and procedures for involvement of U.S. persons in transactions involving embargoed destinations and carefully monitors the access of non-U.S. nationals to information and technology. Controls also are needed for computer networks, especially where ITAR-controlled technology is involved, as well as for transfers of data among affiliates, between R&D partners, and for collaborations with other companies.

Implementing Modern Best Practices

Best practices are constantly evolving and vary from company to company. But certain elements tend to apply. Although not a complete listing, a good export compliance program takes into account the following elements:

- ***Knowing Your Products.*** A proper compliance program requires significant input from personnel with a good familiarity with the technical parameters of the products and their components. Companies need to put procedures in place to ensure proper classification of items on the Commerce Control List, so that they have proper controls on exports for items that have more than 10% U.S. content by value or that for some other reason are restricted. Financial institutions need to evaluate their

products and operations carefully to determine which areas present the greatest compliance risks.

- ***Moving Beyond the Company.*** Traditionally, companies viewed compliance as being complete when the product went out the door or when a financial transaction was complete. No longer. Exporters today need intimate knowledge about their freight forwarders, shippers, agents, and distributors. With the U.S. government aggressively going after transshipment and re-export, they are all part of the risk profile, and need to be integrated into compliance. Similarly, OFAC believes that financial institutions will carefully vet counterparties and other entities involved in financial transactions.
- ***Expanding Due Diligence.*** With internet and computerized databases providing vastly increased research possibilities, the government's expectation that exporters and financial institutions "know their customers" takes on increased urgency. Exporters need to look beyond the actual destination entity and take into account all affiliations and cross-ownership of companies that might reveal suspect end users or re-export risks. With OFAC now treating an entity that is 50% or greater owned by a blocked person as itself blocked,[11] the importance of due diligence is magnified and often requires more than just use of automated computer checks.
- ***Quickly Updating.*** Traditionally, many companies updated their compliance programs quarterly, to take into account changes on the OFAC lists of SDNs and Blocked Persons; the BIS List of Denied Persons, Entity List, and Unverified End-User List; and the DDTC List of Debarred Parties. This would be considered slow today, as it allows too much leeway for inadvertent violations. The best practices is to include nearly real-time incorporation of changes, not only of blocked persons, but also of changes to laws and regulations.
- ***Licensing Exceptions and Opportunities.*** Finally, it should not be forgotten that there sometimes are legitimate ways to engage in otherwise prohibited transactions. These include situations where an export might be allowed under *de minimis* content rules, exceptions for exports of medical and agricultural products to certain destinations, and use of the Validated End-User program, which allows the export of some kinds of controlled items to approved companies in China and India. A well-run compliance program identifies and allows the use of these exceptions where available.

[11] *See* OFAC, *Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked* (Feb. 14, 2008), *available at* http://www.ustreas.gov/offices/enforcement/ofac/programs/common/licensing_guidance.pdf.

Elements of a Well Run Compliance Program

Ensuring compliance with export control and sanction regulations has seven basic steps:

- determining whether the shipment or sale raises concerns about embargoed destinations, suspect users, or re-export risks;
- determining which agency has jurisdiction and which set of export-control regulations is applicable;
- determining the proper classification of the product and what type of export authorization is required;
- determining whether there are destination or end-use controls that would prohibit or restrict export;
- determining whether special export authorization is required and obtaining same;
- monitoring the export to ensure that it is completed in accordance with the terms of authorization; and
- maintaining all required records for the required period or longer.

A proper compliance program deals with all of these elements. A company cannot create a decent program in isolation. A program only is effective if it is tailored to the company at issue, based upon a careful assessment of the risks posed by the company's business activities. This includes an evaluation of where the company does business, its particular product line, the technology it relies on and incorporates in its products, and how it shares technology among business units and outside collaborators. Also relevant is the company's information technology infrastructure and how it can control access to controlled information, its distribution process, its customers, and the company's history of compliance. Companies should consider not just their export control and sanctions risk profile, but also whether they have run into trouble in other areas, such as for FCPA or import violations, which could indicate a careless corporate compliance culture.

The key element of a good compliance program is a well constructed compliance manual. The manual should include a strong statement from senior management that export control and sanction compliance is the responsibility of everyone in the company. It should accurately summarize the laws, using plain language even employees without any legal training can readily follow. The company should distribute the manual to everyone in the company. Many companies require their employees to sign a certification stating that they have read the manual and understand their compliance responsibilities.

Companies should respect certain principles should in compliance programs. A company should:

- Apply a uniform standard across the company for all divisions and countries of operation, unless there is an explicit reason to do otherwise.12
- Promulgate a clear policy that takes away decision-making in "gray areas" from employees who are not experts in export controls and sanctions and gives it to people, either at corporate headquarters or in the general counsel's office, who are well versed in the laws and regulations.
- Provide comprehensive training, which should be given to all new hires and regularly supplemented, at least for key employees who are more likely to confront sanctions and export control issues, such as people involved in contract negotiations, sales, and shipping.
- Require employees to sign an acknowledgement that they have received training and are committed to compliance with all applicable regulations and company export-control and sanction policies.
- Prepare a written compliance policy that includes both a recitation of the law and real-world examples that are relevant to the industry and business.
- Create routine systems that catch most errors while avoiding mechanical over-reliance on systems where common sense would indicate further inquiry.
- Prepare procedures in advance for dealing with questions about potential problems.
- Develop procedures to ensure the retention of all due diligence compliance actions.
- Set up a structure for deciding whether potential problems exist with decisions made by people who are independent of the transaction and who have no pressure to approve suspect transactions.
- Establish procedures where employees can, without fear of retaliation, confidentially report suspected problems.
- Establish procedures to evaluate potential violations and to investigate them.
- Preserve a record of complaints received and how they were resolved.
- Set up a system to discipline individuals who have willfully violated the compliance program and put in place procedures to prevent recurrence of the issue.

[12] Although some export control and sanction laws allow affiliates of the company, such as subsidiaries, to engage in conduct that is forbidden to a U.S. company itself, extreme care must be used when taking advantage of these exceptions because they often have stringent requirements, such as no involvement by any U.S. person at the company.

- Conduct periodic self-assessment of risk and audit procedures to flag areas for improvement.

Most large corporations use intranets to disseminate information efficiently. Best practices include putting basic training online, to allow more people to be trained; providing plain-language summaries of applicable laws; providing lists of real-world examples and frequently asked questions; consolidating all required forms and checklists; providing links to the EAR, ITAR, and OFAC regulations; providing the company's compliance program; quickly disseminating updates to the regulations; informing people about changes in products and technology that could impact the exportable status of goods; setting up links to allow ready reporting of potential problems; and reporting on the resolution of tricky issues. Basically, the intranet can be used as a mechanism to identify problems quickly, report potential issues, and coordinate all of the company's sanctions and export-control policies.

Equally important is to avoid common pitfalls that can trip up even well meaning companies. Common errors include:

- Implementing a compliance program without adequate oversight by the board of directors or a visible commitment by senior management.
- Providing inadequate resources—staffing, information technology support, training funding, funds for consultants or outside counsel—to develop and implement the program.
- Implementing a program that is not well tailored to a company (generally, either implementing one that is too complex to be easily understood or follow, or implementing one that is too legalistic, without clarification from real-world examples).
- Failing to follow up time-of-hiring training with periodic (generally annual) updates to allow refreshment of compliance procedures and communication of new policies and regulations of the agencies.
- Failing to allow for regular auditing to check on the performance of the program.

Increasingly, companies are choosing the cautious approach of redundancy. Traditionally, companies would check customers against denied person lists once—at the time the customer was acquired, when the product or technology was shipped, or when the financial transaction was completed. But today's best practice is to check at multiple set points—a task made far easier by the ease of tapping into the capabilities of interdiction software. At a minimum, companies generally check at the time an order is received or the financial transaction requested, when an order is shipped or the financial transaction completed, whenever an additional party involved in the transaction is discovered (bank, insurance company, freight forwarder, beneficial owner, beneficiary, etc.), and whenever there is an update of any denied person lists. It also is a good idea to run a check of the entire customer base against the denied person lists at least once a year. This allows the firm to be pro-active and flag potential problems even in the absence of any current order

activity.

Compliance is a full time job, and most companies that regularly deal with these issues have a person whose entire job is to keep the company's policies and training up to date. The person or committee in charge of compliance should, at a minimum, take care of the following:

- Providing guidance to management and the different departments within the company on compliance matters.
- Monitoring legal and regulatory developments and best compliance practices.
- Recommending changes to the company's compliance procedures based on such developments.
- Providing for training on compliance issues sufficient to ensure compliance with U.S. regulations and company policy.
- Identifying products, data, and services that are controlled under the ITAR and the EAR and ensuring their proper classification on the USML and the CCL.
- Overseeing the preparation of DDTC, BIS, and OFAC licensing applications and other required paperwork.
- Ensuring compliance with the terms of any licenses.
- Overseeing periodic reviews (preferably annually) to determine the company's fealty to its procedures, updating company policies to reflect any changes in applicable laws, regulations, and agency guidance, and verifying that record retention is in accordance with all applicable requirements.
- Investigating potential violations to determine what happened, whether there is a violation, whether disclosure is needed, and what corrective actions the company should take.
- Providing notification to the company's board of directors and senior managers of any violations.
- Overseeing the proper treatment of blocked assets and their reporting to OFAC.
- Overseeing any required voluntary disclosures or dealing with government investigations.

No compliance program can succeed without proper training. Training methods should, at a minimum, include: (1) orientation for new employees; (2) formal training materials, in the form of a compliance manual, frequently asked questions, and intranet resources; (3) circulation of written memoranda and e-mails as situations arise and are solved; and (4) refresher courses, which should be conducted at least annually. Proper training in the use of the interdiction software, including how to follow up on red flags, is essential. Companies should have

procedures in place to disseminate changes in laws or regulations to relevant personnel as quickly as possible. Companies also should keep records of all training conducted in case they need to be produced in an investigation or disclosure to show the company has been careful in discharging its export responsibilities.

Another consideration is the involvement of a company's human resource department. In many situations it is necessary to identify foreign workers, which often makes interaction with people in human resources important. A good compliance program will institutionalize this system and avoid ad hoc consultations.

The same is true of information technology personnel, who may be involved in blocking technology or information on shared networks or databases. In situations such as this, many companies will implement a technology control plan to systematize identification and segregation of controlled technologies, whether found on computer systems, in R&D laboratories, or elsewhere in the workplace. Technology control plans will typically include a description of the controlled information which the person can, and cannot, access, procedures for limiting access to restricted information, procedures for monitoring compliance with the plan, and requirements that the foreign national sign a certificate evidencing understanding of U.S. Government access requirements. Such measures can avoid the requirement to get a formal license that otherwise would be needed to allow the non-U.S. employee access to controlled technology.[13]

Companies should give consideration, as well, to record retention. Companies should have procedures to ensure that all documents relating to controlled shipments are properly retained, including purchase orders, invoices, shipment (AES) records, airway bills, and other export transaction documents. They also should maintain documents relating to each transaction, such as email, correspondence, contracts, and any due diligence. Where shipments are made under a license, these records should be linked to the license and used to monitor fealty to the license's requirements.

OFAC compliance, too, requires detailed records. Companies should document all checks on new and existing customers, checks relating to setting up accounts, or due diligence on high-risk transfers like extending letters of credit or completing wire transfers. Companies should use interdiction software that is set up to keep automatic audit trails. Institutions also should maintain records needed to prepare annual reports regarding blocked accounts.

[13] An additional issue, often ignored, is that employees in the information technology department generally have ready access to all information on a company's systems. This means that the employment of a non-U.S. person or dual national in the information technology department, in and of itself, can violate export control laws unless procedures are in place to prevent that access or to get the necessary licenses.

Traditionally, most effort was put into implementing the compliance program, with little thought given to spot-checking its effectiveness. The best practice, however, is to implement periodic self-assessments of risks and audits. While this is partially driven by the increasing Sarbanes-Oxley focus on corporate controls requirements, it also makes sense from a pure export-control perspective. Policies well designed in theory can be poorly implemented and there is a tendency for compliance to go onto autopilot. Periodic audits can curtail these problems before they begin.

Most companies therefore should conduct an independent review of compliance at least annually. In performing this review and testing, the company should: (1) perform transaction testing designed to ensure reasonably that the institution is following the ITAR, the EAR, and the OFAC Regulations; (2) review processes to assess employees' knowledge of regulations and procedures; (3) review written procedures and training programs for completeness and accuracy; (4) compare written procedures to operational procedures, to make certain that procedures are being followed; (5) either randomly sample or 100 percent verify the accuracy of export or financial transactions; (6) evaluate whether changes to relevant regulations have been promptly reflected in the compliance program; (7) confirm that correct export authorizations are consistently used for each transaction; (8) confirm that all required documents are properly stored, and in the proper format; (9) review each transaction where a stop or hold was required to confirm that the decision to review was carried out as expeditiously as possible; (10) review records of past audits as compared to current procedures to determine that earlier problems have properly been rectified; and (11) report findings to the company's audit committee. The review can determine risk areas before violations can occur and help ensure that all policies, processes, and procedures of the program are being followed. A written report of the results of the audit should be reviewed by top management and potentially the Board of Directors.

CONCLUSION

Companies sometimes balk at the costs of a proper compliance program, viewing these costs as resources better spent on gaining new business or running the corporation. But it should not be forgotten that the costs of responding to government investigations or conducting internal investigations is extremely high. Criminal and civil penalties can reach into the hundreds of millions of dollars, and that is not even taking into account the costs of debarments, exclusions, or other sanctions available to the agencies. Publicity, too, can be a factor, as many partners are wary of doing business with companies that are viewed as export-control and sanction violation risks. Starving compliance efforts of adequate funding and attention may seem to make sense in the short term, but it is a risky strategy that can come back to haunt a company. When a company is involved in the all-encompassing hassle of an investigation, money previously saved by shortchanging compliance efforts can look like a downright foolish saving.

Author

Gregory Husisian
Of Counsel
Foley & Lardner LLP
202.945.6149
ghusisian@foley.com

APPENDIX: Export Control and Sanction Red Flags

EXPORT-CONTROL RED FLAGS

In evaluating export and sanction risks, companies should keep in mind that the following are the most commonly cited violations of the export-control regulations:

- Improperly classifying products.
- Exporting or re-exporting without appropriate export authorization.
- Furnishing a defense service without proper authorization.
- Allowing access to computer networks without sufficient controls.
- Making false statements to the U.S. Government in connection with a transaction.
- Exporting in violation of a denial order.
- Exporting or re-exporting to embargoed destinations or to prohibited end users.
- Violating the conditions of approval.
- Failure to sufficiently investigate customers and avoid obvious problems.
- Dealing with non-U.S. employees.

To help preventions such as these, the DDTC, BIS, and OFAC have published red flags—suspicious circumstances that should reasonably put a company on alert that there is a chance for an export control or sanctions violation. Practitioners who regularly practice in the field have expanded on these. If any of the following arise, a company should resolve its concerns before entering into, or completing, a transaction.

Shipment-Related Concerns

- The final consignee is a trading company, freight forwarder, export company, or other entity with no apparent connection to the purchaser.
- Delivery dates are vague, or deliveries are planned for out-of-the-way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.

Order-Related Concerns

- The customer is willing to pay cash for a high value order rather than using a standard method of payment.

- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The end-use information provided is incompatible with the customary purpose for which the product is designed.
- The product is inappropriately or unprofessionally packaged.

User-Related Concerns

- The customer appears on one of the blocked person lists: the BIS Denied Persons list, the BIS Unverified list, the BIS Entity list, the OFAC SDN list, the DDTC Debarred list, or the DDTC Nonproliferation list. The current lists can be found at www.bis.doc.gov/ComplianceAndEnforcement/ListsToCheck.htm.
- The customer or ultimate end user is unknown
- Financial information about the customer is unavailable.
- The customer is willing to pay well in excess of market value for the shipment.
- When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for re-export.
- The purchaser is reluctant to provide information on the end use or end user of the product.
- The customer appears unfamiliar with the product, its application, support equipment, or performance.
- The customer orders products or options that do not correspond with its line of business.
- The customer has little or no business background.
- Firms or individuals from foreign countries other than the country of the stated end user place the order.
- The customer declines the normal service, training, or installation contracts.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The customer's order seems inappropriate, such as an order for a replacement part for an item that the customer never ordered.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.

- Routine installation, training, or maintenance services are declined by the customer.
- The customer or its address is similar to one of the parties found on agency lists of denied persons.

Destination-Related Concerns

- The order is being shipped using circuitous or economically illogical routing.
- "Fragile" or other special markings on the package are inconsistent with the commodity described.
- The customer or its address is similar to one of the parties found on a blocked list of denied persons.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The end-destination is Iran, Sudan, North Korea, Cuba, Burma, Syria, or another country with OFAC or BIS restrictions.

RED FLAGS FOR FINANCIAL INSTITUTIONS

Special consideration needs to be given to red flags for financial institution. Primarily, these red flags come up in the context of sanctions. This does not mean that export control issues cannot occur for financial institutions. Investment banks could come across ITAR-controlled information in the context of mergers or acquisitions, banks could be dealing with encryption to safeguard secure transactions, and financing of defense services also could potentially raise ITAR issues, among other potential issues. Nonetheless, the most common issues arise with regard to sanctions, given the focus of sanction programs on access to, and movement of, funds.

In thinking about red flags, it is useful to keep in mind the most common sources of OFAC violations by financial institution. These include:

- Failure to block a transaction despite an explicit reference to a targeted country or SDN.
- Failure to establish an OFAC compliance program.
- Failure to follow the requirements of an OFAC compliance program, or to support it with adequate resources
- Failure to acquire sufficient or proper customer identification.
- Failure to check for SDNs when setting up an account or as part of a requested transaction.

- Failure to block transactions, or to refuse transactions, that involve a designated customer or recipient of funds.
- Failure to retain supporting documentation for a blocked transaction, or to retain it for the full five-year period required.
- Failure to conduct periodic or sufficiently rigorous independent testing for compliance.

Covered financial institutions should give special thought to how they will deal with the following types of red flags:

New-Account Concerns

- The customer refuses to provide information normally required, such as verification of identity, information regarding the source of funds, or other typical know-your-customer guidance.
- Customer attempts to set up multiple accounts and then makes deposits in them that aggregate to more than reporting thresholds, but individually are less than those thresholds.
- Customer provides unusual or suspicious identification documents,
- The new customer provides information that does not check out, that is difficult to verify, or that is downright misleading.
- The customer is reluctant to provide information about the nature and purpose of its business or its business location.
- The customer cannot provide a working telephone contact.
- The customer requests signature authority for multiple people who seem to have no relationship to each other, whether by family or business ties.
- A new account application appears to be connected with an entity on a designated list.
- Requests to set up accounts in countries where local laws or regulations preven tor limit the collection of client-identification information.

Existing Account Concerns

- An account receives large or unusual deposits, interspersed with periods of dormancy.
- A dormant account suddenly receives a large deposit or series of deposits, followed by quick cash withdrawals that remove the added money.
- Cash deposits or withdrawals, especially in large quantities, from a business entity that normally would be expected to deal with checks, payment instruments, or wire transfers.
- Multiple transactions, particularly in cash, where the customer attempts to use different tellers at the same branch of a financial institution.

- Requests for repeated international wire transfers, when it does not appear that business reasons would support such a request.
- Multiple deposits by different individuals at the same branch.
- Consistent pattern of deposits or withdrawals of cash in amounts that are just below reporting thresholds, especially if there seems to be a conscious desire to do so (e.g., the individual presents cash but, after finding out that it exceeds the threshold amount, requests to deposit less so that the threshold is not exceeded).
- Deposits in amounts that do not make sense given stated occupation of the individual (i.e., large deposits from a student).
- Cash withdrawals by the same individual at different branches.
- Customer attempts to persuade a bank employee not to file a required regulatory report regarding customer information or suspicious activity.
- Customer uses an ATM machine to make large bank deposits, especially if of cash or of amounts that are just below threshold reporting requirement.
- Frequent deposits of checks or money orders with sequential numbers.

Fund Transfer Concerns

- Movement of funds at a level that is beyond the expected business or personal income level of the person or entity that owns the account.
- Requests to move funds to or from an offshore bank.
- Requests to wire funds to suspect countries or designated entities, especially if there appears to be no valid business reason or doing so is inconsistent with the customer's stated business or previous history.
- Wire transfers, particularly if for large quantities, from foreign sources where there is no valid reason appearing for them.
- Unexplained wire activity, especially if it is repetitive or shows unusual patterns.
- Large volumes of cashier checks, wire transfers, or money orders, into or out of an account, when the account holder does not appear to have a reason for such activity.
- Unusual or unexpected transfers of funds between related accounts.
- Frequent transfers of funds among multiple banks, such as moving funds from Bank A to Bank B and then back again.
- Frequent requests for withdrawals of large dollar denominations, particularly if paid for by small-dollar deposits.