msk

customs update: compliance? what compliance?

Journal of Commerce

May 21, 2007

LOS ANGELES -- It is impossible to read the trade press, and sometimes even the general press, without thinking, where is that company's compliance program?

In no particular order of significance, but certainly getting many headlines, there is the recent ITT Corp. settlement with the Department of Justice, for a staggering $100 million. The case involved military night vision equipment. ITT sent classified materials overseas without proper authority. Why? Because a few folks (okay, likely lots of individuals) ignored the rules. What happened?

The government charged ITT exported defense-related technical data to China, Singapore and the United Kingdom without first obtaining an appropriate license or written authorization from the State Department. ITT also omitted critical information from Arms Exports Required Reports. Finally, ITT failed to take significant and timely corrective action. Imagine how much worse would have been the outcome if the company had not self-reported to State? ITT pleads guilty to two violations of the 1976 Arms Export Control Act; pays a $2 million criminal fine; a $50 million deferred prosecution penalty and forfeits $28 million as the proceeds of its illegal actions. In addition, ITT pays a fine to State of $20 million.

The $50 million deferred penalty will be suspended for five years. ITT may reduce it on a dollar-for-dollar basis by investing toward the acceleration, development and fielding of the most advanced night vision technology. In other words, State assumes at least some of this technology fell into the wrong hands and is giving ITT the ability to make the existing technology obsolete. What is most intriguing about the settlement is that there was no debarment, or export ban. Typically with a case of this significance, State (and Commerce) would be expected to ban the company from exporting for a period of years. The thinking is this did not happen with ITT since it has such a prominent place in the night vision equipment field. Put another way, State thought its highest priority after punishing ITT was to get better night vision equipment.

practice areas

international trade

regulatory

Why did ITT send the written materials to others? Because it was outsourcing production of some components to a firm in Singapore in order to reduce cost and increase profit. In turn, that firm farmed work out to companies in China and Britain. As a result of this mess, federal enforcement officers are expanding their scrutiny of outsourcing by all defense contractors.

As the name implies, night vision technology enables our military (and others) to see clearly at night. The recent Hamas-Israeli conflict resulted in a sort of tie. Some have suggested that is because Hamas obtained night vision equipment, which is not to suggest it came from ITT. The Iraq war is another example where the military quite rightly wants to make sure the insurgents do not have access to our highly sophisticated equipment. Plus, of course, there are always concerns about the ever-growing Chinese military.

There was apparently some evidence that ITT internal compliance officials warned others not to violate the export regulations but were ignored. Justice clearly painted ITT as a company where some decision-makers put profits ahead of compliance and national security.

The night vision equipment is one of many examples that are causing a clash between military needs and export regulations. Recently, there have been reports the American military in Iraq is finding itself in the position that it cannot give certain equipment to coalition forces as U.S. export laws bar such action. As a result, American military personnel must continue to fight in areas where it wishes to turn over more responsibility to others.

We all heard about problems at Boeing springing from the jet maker improperly using information belonging to rival Lockheed to gain government procurement contracts. In the end, Boeing paid $615 million to settle criminal and civil charges. The company's reputation took a severe hit, as senior executives were sentenced to federal prison, and the company lost $1 billion worth of aerospace launches, was denied certain export licenses, and faced other export bans.

Against that backdrop, one may ask, what was senior management at banana importer Chiquita Brands thinking?

Recently, Cincinnati-based Chiquita agreed to pay a $25 million fine to settle a long-standing Justice investigation into whether it knowingly paid protection money to Colombian paramilitary and rebel groups designated as terrorists by the United States. The company's explanation was it paid the money in order to protect its people and facilities in volatile parts of the country. That defense makes sense and was valid when the payments started in 1997. It was not until 2001 the recipient was declared a foreign terrorist organization and a specifically designated national. Management did not learn this fact until 2003 (which begs the question -- why not?), and following a board meeting, it disclosed the payments to Justice. Executives came away from that meeting feeling Chiquita would not be pursued for prior payments, but its Colombian entity continued making those payments. It was sold in June, 2004. In an ironic twist, Colombian authorities mentioned the possibility of seeking criminal charges against senior executives for approximately $1.7 million in payments.

Clearly one can sympathize with Chiquita wanting to protect its people and facilities, but was this the right way to do it? What did its compliance program require? Did its compliance program even cover this topic?

Next, let's turn to the False Claims Act. In United States v. Merck-Medco Managed Care. L.L.C., 336, F.Supp.2d 430, E.D.Pa. 2004, a federal court held the failure to have a proper compliance and ethics program which is effective under applicable legal standards and industry practices can be the basis for a False Claims Act claim. This approach was based on the concept that the failure to have such a plan in place can lead to the filing of claims paid by the federal government which are "knowingly" false.

In order to prove top management knew or should have known what was going on, Justice had to establish a level of intent. Since there was no paper trail, Justice ticked off the elements of an effective compliance plan as articulated in the Sentencing Guidelines:

- establish an effective code of ethics;
- designate specific high-level personnel with direct responsibility for overseeing compliance who have direct access to top management and the board of directors;
- appoint a compliance officer with responsibility for independent investigation and the power to act on matters related to compliance;
- inform employees of the existence and details of the company's compliance program;
- establish a procedure of regular reports to the board concerning internal investigations;
- put in place effective means to monitor, audit and report on compliance, including an anonymous hotline and protection for whistleblowers;
- implement systems to assure reasonable steps are taken to respond to or investigate reported offenses; and
- regularly enforce the company's policies and procedures through corrective action.

Justice successfully argued that since Medco did not have such a compliance program in place, it acted in reckless disregard of the truth or falsity of the claims made to the government and so was liable for their falsity.

Finally, for purposes of this column, there is the Foreign Corrupt Practices Act. It applies to publicly traded companies only. In its simplest terms, FCPA bars bribes, i.e., payments made by companies to government officials to get deals or favorable treatment. There is a huge difference between presenting a token gift and one which is clearly intended to "grease the wheels" to get a desired deal. We are already beginning to hear stories of prosecutions against American nationals for bribery actions which occurred in Iraq. For those of us old enough, we recall the bribery acts which impacted the aircraft manufacturers some 30 or so years ago.

In each of these cases, one has to ask the question: where was the company's compliance program? Was it robust enough to identify the problem and head it off before it became something that could be called "betting the company?" How did management respond when faced with the actions on which Justice relied? What remedial action was put in place? Did the company disclose its violations to the relevant agencies?

True, each of the situations discussed involves large multi-national companies. Equally true is the fact that when dealing with international trade issues, none of the agencies with jurisdiction make a distinction between large and small companies. Compliance is compliance and if you do not have an adequate program in place, you will get nailed! The federal government will find out, even if it comes from one of your competitors, and your competitors reporting your transgressions is a procedure recognized in the law as a qui tam action. Maybe we'll talk about that basis for action in another column. For now, just how good is your compliance program? When was it last tested by you? When was it last updated?

los angeles
t 310.312.2000
f 310.312.3100

new york
t 212.509.3900
f 212.509.7239

washington, dc
t 202.355.7900
f 202.355.7899