



Penalties are harsh for violating import/export regulations such as ITAR in aerospace and defense electronics

By John McHale

August 2010

Import/export compliance for defense suppliers is becoming almost as complicated and risky as designing defense systems themselves.

Companies must to comply with a variety of import/export regulations such as the International Traffic in Arms Regulations -- better known as ITAR and regulated by the U.S. Department of State -- and the EAR or Export Administration Regulations, managed by the Department of Commerce.

For example, companies that develop electronics listed on the U.S. Munitions List must obtain a license from the State Department before it can be exported. Failure to comply with these regulations could result in business-crippling fines and even jail time for individuals who purposely violate them.



“Fines for ITAR violations in recent years have ranged from several hundred thousand to ITT Corp.’s \$100 million fine” in 2007, says Kay Georgi, an import/export compliance attorney and partner at the law firm of Arent Fox LLP in Washington. “Willful violations can be penalized by criminal fines, debarment – both of the export and government contracting varieties – and jail time for individuals.”

The biggest case right now in the news involves BAE Systems, fined \$400 million by the State Department for violations of the Foreign Corrupt Practices Act, says Lizbeth Rodriguez, OF counsel attorney at Holland & Hart, LLP in Denver, Colo.

BAE Systems and a \$400 million fine

According to a U.S. Department of Justice announcement, BAE Systems plc (BAES) pled guilty in U.S. District Court in Washington “to conspiring to defraud the U.S. by impairing and impeding its lawful functions, to make false statements about its Foreign Corrupt Practices Act (FCPA) compliance program, and to violate the Arms Export Control Act (AECA) ITAR. BAES was sentenced to pay a \$400 million criminal fine.”

It should be noted that none of the criminal conduct described in the plea involved the actions of BAE Systems Inc., a U.S. subsidiary of BAE Systems headquartered in Rockville, Md.

Essentially BAE Systems violated the anti-bribery provisions of the FCPA and other anti-bribery regulations, according to the Justice Department release. “According to court documents, the gain to BAES from the various false statements and failures to make required disclosures to the U.S. government was more than \$200 million.”

According to the Justice Department release “BAES made a series of substantial payments to shell companies and third party intermediaries that were not subjected to the degree of scrutiny and review to which BAES told the U.S. government the payments would be subjected. BAES admitted it regularly retained what it referred to as ‘marketing advisors’ to assist in securing sales of defense items without scrutinizing those relationships.

“BAES admitted that it established one company in the British Virgin Islands (BVI) to conceal its marketing advisor relationships, including who the advisor was and how much it was paid; to create obstacles for investigating authorities to penetrate the arrangements; to circumvent laws in countries that did not allow such relationships; and to assist advisors in avoiding tax liability for payments from BAES,” according to the Justice Department release.

Business BAE Systems conducted in with the Kingdom of Saudi resulted in violations of their arms export licenses, as required by the AECA and ITAR, according to the Justice Department release. The AECA and ITAR prohibit the export of defense-related materials to a foreign national or a foreign nation without the required U.S. government license.

As part of its guilty plea, BAE Systems has agreed to maintain a compliance program to cover all the regulations it violated and to retain an independent compliance monitor for three years to assess the company’s compliance program and to make a series of reports to the company and the Justice Department, according to the Justice Department release. For more information on this case, visit www.doj.gov.

Too much enforcement?

Some company leaders believe the headline-making fines, the increased number of enforcement officers, and myriad complicated compliance regulations are hampering U.S. companies in competing for foreign business.

There has been a great deal of enforcement in recent years and “I’m aware that some feel that it might hamper U.S. business, but I think we don’t do enough when it comes to enforcing compliance.” Protecting U.S. technology is critical to national security, says Dean Young, facilities security officer at Celestica Inc. in Austin, Texas.

Compliance procedures can slow the pace of business, but not complying can shut a business down completely, he notes.

The culture needs to change to doing everything one can to comply as opposed to doing everything one can to avoid it, Young says. “We’re jumping through hoops to get things right so we don’t end up on the front page of a newspaper as a company that has just violated our export laws.”

“While it was a huge argument at the passage of the FCPA in 1977 that such a law would impair U.S. companies in their competition for business in the international arena, I would argue that time has shown that not to be true,” says John Hanson, executive director of Artifice Forensic Financial Services, LLC in Washington. “Companies will still contend so and the point may, in some instances, have some merits, but with the increased passage and enforcement of anti-corruption/bribery laws by other countries – enforcement of those laws is now a trend -- the playing field is even further leveled.

“One thing to be sure, the risks and costs associated with FCPA violations is huge and must be taken seriously,” Hanson continues. “The costs of losing a particular contract because one fails to pay a bribe to gain an unfair advantage in obtaining it is not worth the costs associated with getting caught doing it. What’s to stop a competitor, foreign or domestic, in such an instance reporting an alleged violation to authorities?”



Compliance can slow the speed of business, but the losses from a business can suffer from non-compliance argue for the cautious approach, Rodriguez says.

“The Obama Administration recently launched an interagency review of U.S. export controls laws, the Export Control Reform Initiative, with the objective to reform the current U.S. export control regime,” Rodriguez says. The interagency review is currently in Phase I and most likely it will be a few years before the full scope of the proposed changes is approved and implemented, she continues.

Amending compliance regulation and enforcement

“The main development is the export reform initiative which is still underway,” says Kay Georgi of Arent Fox. “This reform could create a single control list, a single licensing system, and a single agency. That said, while the current administration appears to be working most diligently on the reform effort, it is too soon to tell what the reforms will bring.

“While the full scope of the reform is unknown, the first real regulation to be issued is likely to be a regulation that should benefit companies, particularly foreign companies, that are parties to Technical Assistance Agreements (TAA) and Manufacturing License Agreements (MLA),” Georgi says. “Those companies currently have to identify all dual national and third country national employees who will work on the TAA or MLA or have access to the ITAR technology, including finding out information relating to past citizenships and country of birth. Obtaining such information can raise concerns under foreign anti-discrimination and privacy laws, however. It is expected that the new ITAR regulations will ameliorate this problem although we won’t know until the new rule is issued how far it will go.”

Amendments are also being proposed for the U.S. Sentencing guidelines by the U.S. Sentencing Commission related corporate compliance and monitors.

“I don't think that these changes will in particular affect enforcement, but may spur an even faster increase in the usage of monitors pursuant to settlement agreements between government agencies and the offending companies,” Hanson says. “In the world of FCPA enforcement this is not new, with nearly every settlement agreement -- often called Deferred Prosecution Agreements or Non-Prosecution Agreements -- used in such matters over the last few years requiring both remedial measures within the entities corporate compliance program and the use of a monitor to independently verify the entity's compliance with that and other terms of the settlement agreements.”

Hanson was recently appointed as the monitor of a publicly traded government contracting company pursuant to a settlement between them and a federal U.S. agency, he says.

Best practices for avoiding compliance pitfalls

“The most important piece of advice that I would give a company in the instance you propose is to get experienced assistance,” Hanson says. “The laws and regulations are complex, the penalties grave and the enforcement level high -- all pointing to significant risk in this area. Not only does such an advisor assist in preventing problems from occurring, but they serve as a potential mitigating factor should such a problem occur and the government consider how to penalize the company.”

However, many small businesses cannot afford to hire an attorney like Georgi or Rodriguez or a consultant, but still need to keep ahead of ITAR violations.

“Well, you do get what you pay for,” Georgi says. “In my view you are better paying for an experienced team and just using them for the key issues than flying solo. But there are many things you can do on your own -- hire or select in house an intelligent, motivated compliance person and send him/her to ITAR training provided by SIA or ACI or another solid ITAR training program.

“Have your trained person work with an outside expert to set up a good compliance program for your company,” Georgi continues. “Roll out and educate your workforce on the program. Spend some money for an outside audit of your program to identify weaknesses. Correct the weaknesses and train again.

“It's not cheap, but it is affordable,” she adds. “In fact, if you play in the ITAR sandbox, you can't afford not to.”

Rodriguez agrees, and says that “attorney cost should not be an excuse for not setting up compliance programs. There are many affordable training classes available that are taught by attorneys, such as herself and Georgi, and other services providers.”

“Ultimately, an entity cannot control its employees, subcontractors, agents and representatives, who may make a personal decision to do something inconsistent with corporate policy and/or the law, so a company must demonstrate that it has taken and applied reasonable measures (with particular emphasis on the corporate compliance program and internal controls) to prevent, detect, and respond to such problems,” Hanson says.

Dual-use

One of the most confusing issues for experienced and green compliance officers is dual-use, Georgi says.

“Dual-use items are items subject to EAR administered by the Department of Commerce Bureau of Industry and Security,” Georgi says. Generally speaking, if an item is subject to the EAR, it cannot be subject to the ITAR and vice-versa -- although there are one or two small pockets where dichotomy breaks down slightly. But you can take a dual-use item, modify it, and come up with an ITAR item.

Because it is broader there many things to consider when it comes to dual-use items -- it really depends on the situation or case, Young says. Some might believe that since an item or technology is not covered under the ITAR and is available commercially, then it doesn't require an export license or controls. This could result in an item that really is classified as "Dual Use" on the Commerce Control List (CCL) being exported in violation of Export Laws. Careful screening must be done before exporting anything outside the U.S.

E-mail and compliance

Today many companies use global hubs by which to route their e-mail traffic, Young says. This can be a major compliance issue when the hub is outside the U.S., he continues.

For example at some companies, "if you send out an e-mail to a colleague in the next office it is routed through a hub in another country, then sent back to your office," he continues. If that e-mail data subject to ITAR controls in it I just violated ITAR regulations by sending it out of the country." (Our site has its own e-mail server and we prohibit ITAR sent through e-mails).

In all his e-mails Young places the following note at the bottom: “This e-mail and any attached files are Celestica proprietary and may be legally privileged. Do not e-mail export controlled technical data. If you are not the addressee, any disclosure, reproduction, copying, distribution or other dissemination or use of this communication is strictly prohibited. If you have received this transmission in error please notify the sender immediately and then delete this e-mail.”



People really need to be careful when they send emails, “because once you it hit send you have no guarantee where it will end up,” Young says.

If Young has material subject to ITAR controls that he needs to give to a colleague he walks it over on USB stick or puts it on a protected FTP server,

he says.

Electronic information also needs to be protected when traveling overseas -- laptops, cell phones, etc. -- “I tell all our employees that they must assume that all their text messages, e-mails, cell phone conversations, etc., are being recorded,” Young says.

It is also wise for companies to begin considering the danger of social networking sites when doing compliance training, Young says.

It might be advisable to limit activity on company sites to Facebook and LinkedIn unless the employee has undergone extensive compliance training -- what they think may be an innocent comment could be a compliance violation.

“Employees must be careful about providing information to foreign nationals, especially if your company deals with export controlled technology,” Young adds.

Management support

Getting management support for compliance programs is crucial, especially for small businesses, Young says. Company leadership needs to be aware that one fine could sink their entire business, he adds.

A lack of management support can foil a compliance program before it even gets off the ground, Rodriguez says. Too often management is more interested in the bottom line and feels that spending time dealing with compliance will cost them revenue, but the opposite is the case if they get caught.

Management has to commit time and resources to compliance -- it is not just a matter of applying for licenses it also requires detailed record-keeping and investments in training for all employees and senior management, she continues.

At Celestica, compliance meetings (management review meetings) are held monthly with senior management involvement, Young says.

Columbia Tech is a relative newcomer to the world of ITAR compliance, having only entered into the defense industry about two years ago, but with strong support from management on compliance issues, says Richard Schulman, vice president of quality and ITAR technology control office at Columbia Tech in Worcester, Mass., a contract engineering and manufacturing company. They went about it in a conservative, cautious way, hiring a consultant and taking training classes and today compliance issues take up about half Schulman’s business week, he adds.

ITAR compliance is another part of risk management, Schulman says. “We actually have an insurance agent sit in on the risk assessment meetings we have when discussing whether or not to take on a contract based on ITAR risk.

We will not take on projects that would be too risky for ITAR compliance issues such as any military programs enter into the nuclear arena, he continues. That is not where Columbia Tech's core competencies lie and it would be risky to for it to try and comply in such an environment, Schulman says.

Hiring the right compliance officer is also crucial, Young says. "Export Compliance requires a background and understanding of the numerous export/import laws and a constant vigil to ensure your company is always doing the right thing, every time."

This type of individual has an appreciation and true understanding of compliance and how to make sure companies meet regulations and refrain from getting fined, he adds.

Important ITAR links

Lizbeth Rodriguez Of counsel and attorney with Holland & Hart LLP in Denver, Colo., recommends sections of the U.S. Department of Commerce, Bureau of Industry and Security, U.S. Department of Treasury, Office of Foreign Assets Control, and U.S. State Department, Directorate of Defense Trade Controls, websites for those looking to get started with compliance.

For the Export Administration Regulations, visit http://www.access.gpo.gov/bis/ear/ear_data.html#ccl.

For the International Traffic in Arms Regulations, visit http://www.pmddtc.state.gov/regulations_laws/itar.html.

For guidance from the regarding the elements and implementation of an effective Export Compliance Management Program, visit <http://www.bis.doc.gov/complianceandenforcement/emcp.htm>.

For general information on ITAR compliance requirements, visit <http://www.pmddtc.state.gov/>.

For general information regarding U.S. trade sanction programs, visit <http://www.treasury.gov/offices/enforcement/ofac/>.

For several lists of entities and individuals that have been denied export privileges or with whom U.S. parties are restricted to conduct business, visit <http://www.bis.doc.gov/complianceandenforcement/liststocheck.htm>.

For frequently asked questions on Commerce Department export licensing, visit <http://www.bis.doc.gov/exportlicensingqanda.htm>.

For a list of ITAR violation consent agreements going back to 1978, visit http://www.pmddtc.state.gov/compliance/consent_agreements.html.

For a fact sheet of President Obama's Export Control Reform Initiative, visit <http://www.whitehouse.gov/the-press-office/fact-sheet-presidents-export-control-reform-initiative>.

For more information on Holland & Hart's export practice, visit <http://www.hollandhart.com/practice.cfm?IDName=DeptID&ID=198>.