Penalties are harsh for violating import/export regulations

Military & Aerospace, 27 Jul 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. 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. 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, says Dean Young, facilities security officer at Celestica Inc. in Austin, Texas. 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. 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. 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. Source: http://www.militaryaerospace.com/index/display/article-display/6130376019/articles/military-aerospace-electronics/exclusive-content/2010/7/penalties-are_harsh.html