

Failing to Comply with Technology Export Laws May Prove Costly

April 2, 2007

Does your organization ship software or products containing encryption technology to customers, affiliates or trading partners in other countries? Are you in compliance with the many export laws and regulations with respect to those shipments? A failure to comply can result in stiff criminal sanctions.

Recently, ITT Corporation, manufacturer of military night vision equipment, pled guilty to violating the Arms Export Control Act, when it shipped its equipment to China, Singapore and the United Kingdom without first obtaining a license from the U.S. Department of State. ITT earned \$28 million in profit on the illegal transactions and has been assessed a \$100 million penalty as a result of the violations.

It is not just the ITTs of the world that are at risk of violating the complex U.S. export laws. The overseas shipment of software or products containing encryption technology is highly regulated and the unwary may face severe penalties. If your organization is dealing with an entity in another country, this is not an area to "cut corners". The first step is awareness of what is required to send encryption technology to the involved countries. It is strictly prohibited to export certain classifications of technology to some countries, such as Libya and Iran. While exports of the same technology may be allowed to other countries, such as Hungary and Iceland, the regulations may require that you first obtain proper permission.

The best time to determine what those regulations are and how they may impact your business is before entering into a transaction with an entity in another country. Consulting with a legal professional at an early stage can prevent your organization from becoming the subject of the next Department of Justice press release.