The World's Largest Circulation Marine Industry Publication • The Information Authority for the Global Marine Industry since 1939

MARITIME REPORTER AND ENGINEERING NEWS

www.marinelink.com

March 2010

Burgeoning International

Navy Budgets

Maritime Security

Technology vs. Technique

Technical

Integrated Bridge Solutions

Five Minutes With

Karen Hughey, CEO, ABS Nautical

MARITIME REPORTER AND ENGINEERING NEWS

Reprinted from the MARCH 2010 Edition of Maritime Reporter & Engineering News

International Business Regulation in the Shipyard

By Barbara D. Linney, Partner,
Blank Rome LLC

Shipyards and contractors whose operations include both U.S. and foreign government naval and Coast guard programs are required to comply with numerous U.S. federal laws and regulations. Of these, export control laws and regulations and anti-bribery laws in particular have been the subject of steadily increasing enforcement activity.

Export control

The primary sources of export control regulations are the Arms Export Control Act, as implemented by the International Traffic in Arms regulations (commonly referred to as the ITAR), and the Export Administration Regulations (the EAR). The ITAR regulate the export of defense articles, defense services, and technical data listed on the United States Munitions List (USML), while the EAR regulate various commercial items, primarily those that are critical to national security or can be diverted for uses contrary to national security or in support of terrorism. These laws and regulations apply to both domestic and international operations of U.S. shipyards and contractors, and have the purpose, among others, of preventing unauthorized access to export-controlled information by foreign nationals both in the United States and abroad.

While the sending or taking of defense articles or technical data or performing a defense service overseas are commonly understood by most to be export activities subject to controls, many shipyards and contractors still fail to appreciate that under the so-called "deemed export" concept, a release or disclosure of export-controlled information or services to foreign nationals in the United States constitutes an export that requires prior authorization from the applicable export control agency. Another misunderstanding that complicates compliance in this area is the still commonly held belief that technical data is not export-controlled if it is not classified. On the contrary, while it is true that all classified information relating to defense articles and defense services is export-controlled, not all export-controlled information is classified, and several recent enforcement initiatives have focused on unlawful exports of unclassified technical data.

Anti-bribery

Shipyards and contractors seeking or performing work for foreign government customers also must comply with the Foreign Corrupt Practices Act (the FCPA), which prohibits corrupt payments (or offers or promises of such payments) to foreign government personnel for the purpose of obtaining or keeping business. This "business purpose" test is broadly applied, and the corrupt "payment" may be anything of value. The list of prohibited recipients likewise is broadly framed to include foreign political parties and party officials, candidates for foreign political office, and foreign officials – defined in turn to include officers or employees of foreign governments, public international organizations and their departments and agencies, as well as any person acting in an official capacity. Payments may not be made through third party intermediaries, and the recipient need not be the party from whom business is sought.

Recent Enforcement Initiatives

Export control violations can result in both criminal and civil penalties. Numerous recent cases illustrate the importance of vigilance on the part of U.S. government contractors against economic espionage and theft of trade secrets involving export-controlled information, including the case of a former engineer with a U.S. Navy contractor who was found guilty of conspiring with several family members to obtain and illegally export U.S. Navy current and future warship technology to China. Corporations as well as individuals have been subject to criminal penalties for export violations. Civil penalty cases can result in fines and imposition of remedial compliance measures (including compliance monitors and audits), and both criminal and civil penalty cases can lead to suspension or debarment. Although past ITAR enforcement initiatives have tended to focus on larger companies, the last two years have seen a trend towards imposition of civil penalties and related enforcement action against smaller companies. In one such case, a software development company that specialized in creating computer models used for design testing in simulated water and other environments entered into a consent agreement providing for fines and remedial compliance measures after engaging in unauthorized exports of technical data and defense services.

Violations of the anti-bribery provisions of the FCPA are subject to criminal penalties, including fines and imprisonment. Enforcement actions against both U.S. and foreign corporations have resulted in staggering fines, as well as compliance monitoring. Nor are individuals immune from prosecution, as illustrated, for example, by a recent case in which two Virginia men are awaiting sentencing after pleading guilty to charges arising out of a scheme to bribe officials of the Panama Maritime Authority to secure a contract to maintain lighthouses and buoys. The trend towards indictment of individuals for FCPA offenses accelerated in January of this year with the arrest and indictment of 22 employees of military and law enforcement suppliers in connection with an alleged scheme to bribe African government officials. This case is also significant in that it involved a large-scale sting operation claimed by law enforcement officials to be the first of its kind in the FCPA context.

There is also a trend towards convergence of export and FCPA enforcement actions. For example, in a 2008 case, a naturalized U.S. citizen born in China was charged with violations of both the ITAR and the FCPA in connection with the unauthorized export of defense articles and services and related attempt to bribe a Chinese government official. More recently, a Florida man said to have been linked to the FCPA sting operation has been charged with unlawful exports of controlled goods and conspiracy to violate the FCPA.

Breach of Contract

U.S. defense acquisition regulations require contracting officers to include certain clauses in all U.S. Department of Defense solicitations and contracts involving export-controlled items – i.e., defense articles, defense services, and technical data, as defined in the ITAR, and export-controlled commodities, software and technology subject to the EAR. However, the burden of compliance with the ITAR and the EAR remains squarely on the contractor irrespective of whether the clause is included, and even if export-controlled items are expected to be involved in the performance of the contract, the government has no obligation to specifically identify any such items. Thus, rather than providing clarity as to the export compliance obligations of the contractor, the primary effect of this requirement appears to be that contractors may be subject to breach of contract claims in addition to enforcement action for failure to comply with export control laws and regulations.

Compliance – the Best Defense

In view of these risks, shipyards and contractors should become familiar with the EAR and the ITAR in order to determine whether their operations entail use or generation of export-controlled items, and implement compliance programs designed to limit risks associated with regulatory enforcement as well as the breaches of contractual obligations. Shipyards and contractors vying for foreign government business should ensure that their compliance program includes training and procedures focused on both FCPA and export compliance. In addition to serving as the front line of defense against violations, a compliance program may be considered a mitigating factor in both criminal and civil enforcement proceedings in the event that violations do occur.

About the Author

Barbara Linney is a partner in the Washington D.C. office of Blank Rome LLP, practicing in the area of international trade and transactions. She regularly advises both U.S. and foreign clients regarding U.S. export controls and international economic sanctions, defense trade and security regulations, anti-bribery and anti-boycott regulations, and other international trade and business issues, including foreign investment review, mergers, acquisitions and financings. She represents clients before various federal agencies, including the Departments of Commerce, Defense, State, and Treasury (Office of Foreign Assets Control and Committee on Foreign Investment in the United States). Ms. Linney, who holds a masters degree in international law from Georgetown University, also serves as General Counsel to Women in Federal Law Enforcement and the Washington D.C. chapter of Women in International Trade, of which she is a past President. Linney@BlankRome.com