JUSTICE DEPARTMENT PLANS STEPPED-UP CRIMINAL ENFORCEMENT OF EXPORT CONTROL LAWS

U.S. Attorney General Alberto Gonzales recently announced that the Department of Justice (the "DOJ") is launching a "national export enforcement initiative" to investigate and prosecute violations of U.S. export control laws. The DOJ's heightened attention to export control violations should be taken as a signal by U.S. businesses engaged in international sales or transfers of sensitive information or technology - including computers, software, equipment, electronics, or associated intellectual property - that, in addition to incurring significant civil penalties, they could be subject to criminal prosecution for alleged violations. Simultaneously, Congress is considering legislation to increase civil penalties for export violations. Therefore, affected businesses, especially multinational companies, should review and reassess their export control compliance programs to assure that these programs incorporate best practices and promote full compliance with the applicable laws and regulations.

Gonzales spoke at a law enforcement "summit" on Global Initiatives to Combat Nuclear Terrorism and highlighted continuing efforts by terrorist organizations and "rogue states" to obtain from the United States "seemingly innocuous components" - many of which have benign commercial applications - and divert them to military uses, including the development of nuclear devices and other weapons of mass destruction. As an example, the Attorney General cited a recent case involving the illegal export of a medical device used in the treatment of kidney stones that, in the wrong hands, can be used to detonate a nuclear warhead. The DOJ initiative is designed to improve federal government detection, investigation, and prosecution of illegal exports of such "dual-use" and other controlled items and includes special training for federal prosecutors to enable them to undertake such specialized prosecutions.

To implement the national export enforcement initiative, the DOJ will work closely with the three federal agencies that currently regulate export transactions affecting U.S. national security and foreign policy concerns. The State Department's Directorate of Defense Trade Controls regulates the export of the goods, services, and technical data used in military applications that are considered "defense articles" and are included on the U.S. Munitions List ("USML"). The USML includes not only arms and munitions but also communications equipment, electronics, and materials, parts, and components designed or modified for use in military applications.

The Department of Commerce's Bureau of Industry and Security administers the licensing program for exports of sensitive items capable of being used in both civilian and military applications and included on the Commerce Control List of the Export Administration Regulations.

The U.S. Treasury Department's Office of Foreign Assets Control ("OFAC") enforces the current U.S. trade embargoes against Cuba, Iran, and Sudan, and trade sanctions against certain other countries, terrorists and terrorist organizations, as well as narcotics traffickers, drug kingpins, and those involved in the proliferation of weapons of mass destruction. Although the specific prohibitions vary based on the particular program involved, nearly all import, export, financing, trade, and investment with embargoed countries is prohibited unless licensed by OFAC.

In the past, a number of companies have been surprised by the requirements and scope of U.S. export control laws, which govern even intra-company transfers of sensitive items (such as computer software) by a U.S. parent to its overseas subsidiary. Violators are subject to administrative penalties and may also be subject to criminal fines, imprisonment, or both, and these fines may increase under pending legislation. Congress is currently considering a bill (S. 1612) to increase the maximum civil penalty for violations of sanctions and dual-use export control laws from $50,000 to $250,000, or twice the amount of the transaction that is the basis of the violation, whichever is greater. The measure also would boost the maximum criminal fine for an export violation from $250,000 to up to $1,000,000, and raise the maximum term of imprisonment from ten to 20 years.

To avoid such surprises and harsh penalties, U.S. multinational businesses should review their current export compliance programs in light of recommended best practices, test compliance procedures, revise their compliance programs as necessary, and assure that affected personnel at all levels of the business are knowledgeable as to the details and importance of complying with both the letter and the spirit of U.S. export control laws and regulations. Based on recommendations by export practitioners and legal experts, a compliance program designed for maximum effectiveness should incorporate at least the following elements:

- a strong and continuing commitment by senior management that includes active involvement in compliance, clear communication about the program both within the company and with outside contractors, foreign distributors and similar parties, and periodic audits of the program's effectiveness;
- adequate compliance resources that include high-quality senior compliance managers, internal instruction manuals, personnel training, and compliance information disseminated through the company's intranet;
- a screening program to detect potential exports or other transfers that might be prohibited or controlled and to identify prohibited customers, end-users, or countries;
- procedures for managing the necessary export license applications, implementation of license authorizations, and the business's relationship with the federal agency issuing the license;
- proper maintenance and preservation of export-related records; and
- procedures for detecting and reporting suspected violations and appropriate discipline for noncompliance.

These best practices should be adapted by each business to its own operations, based on the nature and scope of its exports, location(s) of operations, customers, and end users, and the level of potential risk.

* * * * * * * * * * * * * * * *

If you have any questions concerning the foregoing, or would like additional information, please contact Russell Smith (202-303-1116, rsmith@willkie.com), Miriam Bishop (202-303-1126, mbishop@willkie.com), or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, D.C., 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, D.C. telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

June 27, 2007