GAO Finds Sensitive U.S. Technology Can Be Exported Easily and Legally

Source: Daily Report for Executives: 06/23/2009

Export Controls

The Government Accountability Office has found through a yearlong undercover investigation that militarily sensitive U.S. technology can be "easily and legally" purchased in the United States and exported to suspect destinations abroad.

Officials with the Commerce Department's Bureau of Industry and Security (BIS) said that they continue to inform manufacturers and other members of the exporting community of their export control responsibilities and to encourage voluntary compliance and the detection of potential violations.

But a leading U.S. law firm—Sidley Austin LLP—has warned U.S. companies that, as a result of the GAO investigation they should expect to see enhanced government export enforcement activities that focus on domestic sales.

Rep. Bart Stupak (D-Mich.), chairman of the House Energy and Commerce Subcommittee on Oversight and Investigations, which ordered the GAO investigation, called the agency's findings "troubling."

"This is obviously not a satisfactory result," Stupak said at a subcommittee hearing earlier this month. "There is an enormous loophole in the law."

Transshipment Point

In testimony at the hearing, Gregory D. Kutz, managing director of forensic audits and special investigations at the GAO, said that the agency's findings were based on an undercover investigation that involved setting up a bogus front company to purchase sensitive items such as night-vision scopes currently used by U.S. soldiers in Iraq and Afghanistan and triggered spark gaps used to detonate nuclear weapons.

Kutz said that the GAO was then able to export a number of dummy versions of the items by mail to a country known as a transshipment point for terrorist organizations and foreign governments attempting to acquire sensitive technology, which he did not name.

He said that enforcement officials in the United States said that it is impossible to search every package and person leaving the country to ensure that sensitive technologies are not being exported illegally.

"As a result," Kutz said, "terrorists and foreign governments that are able to complete domestic purchases of sensitive military and dual-use technologies [that can be used for both military and commercial purposes] face few obstacles and risks when exporting these items."

He said that the undercover investigation was conducted from May 2008 to June 2009.

"When we discussed our covert shipments with State, Commerce, and various law enforcement agencies responsible for monitoring packages, vehicles, and persons exiting the United States," Kutz said at the June 4 hearing, "they were not surprised by our success. Officials from several agencies stated that there is no practical way to ensure that otherwise unsuspicious people, vehicles, or packages leaving the United States that carry or contain export-controlled items can be identified and searched consistently. … [The State Department] agreed that it is difficult to prevent items from leaving the country after they are legally sold to an individual within the United States."

Customer Screening Not Required

Matthew S. Borman, acting assistant secretary of commerce for export administration, said at the hearing that BIS provides "extensive" export control assistance to the business community through its counselling offices in Washington, D.C., and California, which includes educational outreach activities that help facilitate industry compliance with U.S. law. But he said that U.S. law does not explicitly require domestic sellers to screen their customers, although many do so "as a matter of due diligence because of potential liability."

Borman said that companies are aware of the potential liability because BIS works closely with the export trade community to raise awareness of "compliance best practices" and "red flags" of potential illicit export activities, as well as to identify and act on export violations.

He said that the administration is also reviewing the existing law enforcement authorities of BIS special agents to determine if additional

authorities are required to enable BIS to "better address the current security and commercial environment."

The law firm of Sidley Austin LLP, meanwhile, said in an "Export Controls Update" posted on its Web site (http://www.sidley.com/sidleyupdates) on June 17 that the GAO findings will likely lead to "even greater government interest in the control of sensitive technologies."

"Although a legislative solution extending export control requirements to domestic sales is unlikely in the short term (and unpopular with industries facing competitiveness concerns)," the Sidley Austin advisory said, "U.S. law enforcement authorities are anticipated to increase industry outreach. U.S. companies should expect more frequent visits from BIS and other agencies involved in export control enforcement such as the Federal Bureau of Investigation, Immigration and Customs Enforcement, and the Naval Criminal Investigative Service."

The advisory said that requests for cooperation with government investigations, such as through the production of sales records, may also increase. "If such sales records reveal that a U.S. company has been contacted by a suspected front company or transshipper," it said, "the U.S. company can expect to be asked to cooperate by participating in a controlled delivery as the basis for a criminal prosecution. U.S. companies should therefore prepare themselves for this likely increase in outreach. In particular, companies should consider whether their internal compliance procedures with respect to domestic sales effectively minimize the risk of product diversion for illegal export."

The advisory concluded by saying that voluntary implementation of enhanced compliance procedures for domestic sales may reduce the likelihood of government outreach by protecting a company from inadvertent sales to domestic parties intent on illegal export.