

About This Issue

This issue of the *International Law Report* highlights the effect on various industries of the U.S. Government's increased efforts to reduce the threat of terrorist activity.

In This Issue:

Customs Update:

- US-VISIT Program Imposes New Requirements on Individuals Entering the United States

Export Update:

- U.S. Government Focuses on Transshipments and Threats to National Security

Import Update:

- Heightened U.S. Efforts to Protect Imported Food

▪ Editorial Contact

If you have questions, comments or ideas about articles in the *ILR*, please contact the editor:

William T. O'Brien
202.496.7107

CUSTOMS UPDATE

▶ US-VISIT Program Imposes Strict New Entry/Exit Requirements on Foreigners Entering the United States

In early 2004, the U.S. Government began stepping up efforts to track and monitor foreigners within its borders under the United States Visitor and Immigrant Status Technology Program ("US-VISIT"). Any entity that relies upon foreign employees coming into the United States to perform work – from IT workers to truck drivers to executives on business travel - should be aware of US-VISIT, which imposes strict new entry/exit requirements. Moreover, companies that rely upon cross-border shipping (particularly via land) need to pay careful attention to existing and proposed US-VISIT requirements. These requirements could interfere with other programs designed to ease commerce, such as the Customs-Trade Partnership Against Terrorism or the Free and Secure Trade program.

US-VISIT is intended to ensure that the United States maintains accurate information on persons entering or staying within its borders and that entry is refused to individuals who pose a security threat. Under the program, certain vital "biometric" information is collected upon a foreigner's entry into the United States, and upgraded technology is then used to track such persons once in-country. Biometric information is data that is used to uniquely identify individuals by evaluating one or more distinguishing biological traits. Biometric identifiers can include fingerprints, hand geometry, retina and iris patterns, DNA, and signatures. Per US-VISIT procedures, digital fingerprints and digital photos will be gathered.

US-VISIT is a major component of the U.S. Government's so-called effort to "push the border out." The United States intends to collect extensive biometric information

on all persons entering and exiting the United States and use this information overseas in the fight against terrorism. By “pushing out” the border, the U.S. hopes to stop suspicious individuals before they reach U.S. entry points. While US-VISIT will undoubtedly inconvenience legitimate visitors, the U.S. Government’s goal is to balance legitimate security concerns with the need to move legitimate travellers more rapidly through entry points.

Origins of US-VISIT

While the roots of US-VISIT predate 9/11, the events of that day have made the system all the more important. US-VISIT stems in part from the Immigration and Naturalization Service Data Management Improvement Act of 2000, Public Law 106-215 (codified as amended at 8 U.S.C. 1365a). This law amended a previous requirement for an entry/exit system that mandated the recording of the arrival and exit of aliens who crossed a U.S. border, and which was intended to be implemented by the end of 2003. A later law required the creation of a system that would record the entry and exit of every alien admitted under the “Visa Waiver Program”. See Visa Waiver Permanent Program Act of 2000, Public Law 106-396 (codified as amended at 8 U.S.C. 1187(h)).

After 9/11, demand grew for an ever stronger entry/exit system, resulting in the USA PATRIOT Act. See 8 U.S.C. 1379. Under this Act, the U.S. Government was required to develop and certify a new technology standard, including biometric identifier standards, that could be used to verify the identity of visa applicants and persons seeking to enter the United States. The main focus of this new requirement was the use of biometric identifiers and the development of tamper-resistant documents that can be read at ports of entry. In addition, the use of machine-readable, tamper-resistant visas and other travel documents that use biometric identifiers are required by October 26, 2004.

Purpose of US-VISIT

The main purpose of US-VISIT is to establish a method for ensuring that immigrants and visitors are properly tracked as they enter or leave the United States, and that the U.S. government maintains a database system that allows such information to be shared by law enforcement and intelligence agencies. The information gathered will enable the U.S. Government to determine:

- who should be barred entry from the United States;
- who is eligible to have their immigration status adjusted;
- who has overstayed or violated the terms of their admission;
- who should be apprehended or detained for law enforcement purposes; and
- who needs special protection (i.e., refugees).

The ultimate goal of the program is to enhance the security of the United States while facilitating legitimate trade and travel. US-VISIT is overseen by Asa Hutchinson, Under Secretary for Border and Transportation Security of the Department of Homeland Security (“DHS”).

Implementation of US-VISIT

Due to the wide-ranging and ambitious goals of US-VISIT, implementation will be phased in. The collection of biometrics of foreign nationals with visas began in early 2004 at air and sea ports of entry. This biometric information is then cross-checked

against watchlists and monitored for the duration of the visitor's stay.

Access to US-VISIT Information

The information collected through US-VISIT will be made available to a number of different U.S. government agencies, including:

- Customs and Border Protection Bureau officers;
- Bureau of Immigration and Customs Enforcement special agents;
- adjudications staff at the U.S. Citizenship and Immigration Services;
- State Department consular officers, related staff, and attorneys;
- certain members of the U.S. intelligence community; and
- other sections of DHS such as the Transportation Security Administration.

Federal law enforcement officers, such as Federal Bureau of Investigation Agents, may also have access under the USA PATRIOT Act. The DHS Secretary may, in his discretion, disclose US-VISIT information to state and local law enforcement officials. Foreign governments may receive US-VISIT information only when permitted by law and if deemed necessary for intelligence and law enforcement interests.

US-VISIT and the Visa Waiver Program

Currently, persons from the so-called "Visa Waiver Program" ("VWP") countries¹ are not yet seriously impacted by US-VISIT requirements because they are not subject to all of the program's requirements. However, starting in late October 2004, persons from VWP countries will be required to produce machine-readable, tamper-resistant passports that meet certain biometric standards for photographs. An exception will be made if the person's passport was issued before October 26, 2004, and has not yet expired. For any person covered by US-VISIT, failure to provide the proper identifiers at the time of entry could lead to the inadmissibility of the person, although the rule provides some leeway depending on whether the identity of the person can be verified through other methods.

DHS optimistically expects that the additional processing under US-VISIT will only add an average of 15 seconds to a person's screening. But DHS reportedly has alternate plans in place should screening cause significant delays in processing visitors.

Opportunities to Shape or Participate in the US-VISIT Program

Because US-VISIT is still in its formative stages, many opportunities exist to shape its final form. Part of DHS's experimentation includes testing various methods for collecting information, such as the use of self-serve kiosks and hand-held scanners. DHS is also soliciting comments on how best to collect biometric information at the time of a covered person's departure, and is open to comments on any delays or negative effects on travel, trade, commerce, tourism and "desired aspects" of immigration. Providing input is critical because public comments will be considered in future rulemakings related to US-VISIT.

Finally, US-VISIT presents an interesting business opportunity as it is a well-funded portion of the DHS budget. In FY 2003 approximately \$380 million was designated for US-VISIT while \$330 million is set for FY 2004. Considering the broad expansion that is planned for US-VISIT in the near future, opportunities to become involved in

the provision of biometric-related equipment are likely to expand.

Conclusion

US-VISIT is a complicated but critical part of the effort to secure the borders of the United States. Because of the potential impacts on trade and the influx of foreign employees it is important to thoroughly understand this new program.

Should you have any questions regarding US-VISIT, please contact Brian Finch at 202-496-7241.

Brian Finch
Washington, DC

Endnote

1. These include: Andorra, Austria, Australia, Belgium, Brunei, Denmark, Finland, France, Germany, Iceland, Ireland, Italy, Japan, Liechtenstein, Luxembourg, Monaco, Netherlands, New Zealand, Norway, Portugal, San Marino, Singapore, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom (citizens with the unrestricted right of permanent abode in England, Scotland, Wales, Northern Ireland, the Channel Islands and the Isle of Man.)

[↗ Back to top](#)

EXPORT UPDATE

▶ U.S. Government Steps Up Enforcement Actions Against Transshipment of Goods

Cases involving the transshipment of goods have become a major focus of recent export control enforcement actions pursued by federal government agencies. A transshipment occurs when goods or technical data ostensibly intended for one destination are sent to a different destination. Attuned to the potential national security threats that transshipments present, agencies such as the Departments of State, Commerce, and Justice are focusing on the export activities of a variety of companies, including manufacturers of weapons and defense systems; manufacturers, designers, suppliers and distributors of security and energy-related goods and systems; engineering services companies; and suppliers of industrial and scientific machinery and components.

Transshipments can be a troublesome issue for exporters. In many cases, the exporter has received agency approval to export the goods or technical data to one destination but not to the ultimate end-destination. The ultimate destination of the goods, furthermore, is often one for which export approval would have been difficult or impossible to obtain.

Recent Enforcement Actions

Several recent enforcement actions highlight the various ways the U.S. Government is aggressively targeting transshipments:

1. An employee of a U.S. design and engineering firm serving the nuclear, aerospace and light industrial and scientific industries was charged in late 2003 with sending technical data for an atomic energy pressure valve to a major

foreign industrial firm in New York, allegedly with knowledge that the blueprints would ultimately be sent to North Korea. The drawings apparently contained an annotation that they were to be used in a nuclear facility in North Korea. The government contended that the drawings were export controlled, and that the defendant failed to obtain an export license prior to shipping the drawings to its customer. A prior rejection of an application by the defendant to export similar technical data and hardware to India allegedly demonstrated the defendant's familiarity with regulations concerning exports to countries with "unsafeguarded" power facilities. This fact was taken to indicate that the defendant's conduct was intentional and willful. The defendant faces up to 10 years in jail and fines of \$250,000.

2. In September 2003, a U.S. engineering company and its chief financial officer were sentenced for violating the Export Administration Act by exporting laboratory equipment to Pakistan. The company's application for an export license listed a university in Pakistan as the intended recipient. Upon investigation, however, it was determined that an entity controlled by the Pakistani government, and not the university, was in fact the intended recipient. The Department of Commerce (DOC) denied the export license because it was concerned that the equipment could be used for nuclear weapons development in Pakistan. The defendant then shipped the equipment to its German subsidiary for ultimate shipment to Pakistan. Both the corporation and the individual received substantial fines and the individual was sentenced to prison.
3. In July 2003, a number of U.S. businesses were searched as part of a probe into shipments of military hardware to a company in the United Kingdom that allegedly supplies goods to the Iranian military. The nationwide investigation examined 18 companies and resulted in the seizure of records and the indictment of employees. According to certain reports, the companies that sent parts to the U.K. firm allegedly failed to ascertain the end-use destination of the parts.
4. In December 2002, several companies and individuals, including a U.S. manufacturing company and its president, were charged with exporting spare parts for military aircraft without the required State Department license. Although the primary violation alleged appears to be the failure to obtain any export license, the prosecution appears to be presenting the case as one in which the defendants did not take any steps to ascertain the end use of the articles. The case is scheduled to go to trial in the spring of 2004.

The frequency of such cases demonstrates that transshipments are a common peril for exporters and that the government is attuned to the potential national security threats that transshipments present. Enforcement agencies also may be inclined to view transshipments as being indicative of willful intent on the part of the exporter, even where, in fact, an exporter may not know or intend that the exported goods will be transshipped.

Government Initiatives to Control Transshipments

Concern over transshipments has spurred regulators to establish formal initiatives to limit transshipment violations and more closely scrutinize transactions involving key transshipment hubs. This is exemplified in the DOC's Transshipment Country Export Control Initiative (TECI), launched in the fall of 2002. The TECI Initiative seeks to strengthen control of the transshipment trade by strengthening the trade control systems of those companies and territories which are deemed to be global transshipment hubs. Particular targets include global transshipment hubs with large volumes of trade, close proximity to destinations of concern, or those destinations

with liberal export control policies for exports. These include such sites as Panama, Malta, Cyprus, U.A.E., Singapore, Malaysia, Thailand, Taiwan and Hong Kong, though the list can be amended at any time.

The apparent vigor with which regulatory agencies pursue enforcement actions in transshipment cases and the establishment of TECI highlight the importance of exporters knowing both the end-user and end use of all controlled articles that are exported.

At a minimum, DOC has certain expectations for compliance programs relating to export issues, particularly transshipment compliance. Exporters should strive to incorporate these and other best practices into their export compliance programs by tailoring a control program to their unique situation. Such best practices include:

- Developing written policies against allowing exports that contribute to terrorism or to programs of proliferation concern.
- Creating an export compliance program and integrating it with the company's overall regulatory compliance, security and ethics programs.
- Identifying one person as the responsible party for overseeing the company's export control compliance program. This individual should report to the company's chief executive officer, general counsel or other senior management official, but not an officer whose primary function in addition to export control is sales or marketing.
- Taking appropriate steps to know the end-user and determine whether the item will be reexported or incorporated into an item to be reexported, particularly with respect to transactions to, from, or through transshipment hubs.
- Ensuring there are compliance and/or business procedures in place to ensure immediate responsiveness to theft or unauthorized delivery, in particular for transactions to, from, or through transshipment hubs. Procedures should include means to ensure that the exported item reached the proper end-user, such as obtaining documented confirmation.
- Paying heightened attention to what the DOC calls "Red Flag Indicators", or possible violations of the Export Administration Regulations. If suspicious transactions are encountered, exporters should attempt to resolve any questions raised by the transaction. If they cannot be resolved, the company should refrain from the transaction and notify U.S. law enforcement agencies of potential or actual violations.
- Having an express understanding, such as by contract, with suppliers, partners or end-users as to the handling and final destination of the goods in question.

As recent enforcement actions and government initiatives reflect, transshipment poses an area where exporters must carefully scrutinize exports and their procedures for complying with export control regulations. With proper procedures and due care, exporters can seek to avoid the pitfalls of export control violations and the subsequent enforcement actions. For more information, please contact Jason Silverman or Michele Miranda.

Jason Silverman and Michele Miranda
Washington, DC

IMPORT UPDATE

▶ Recent Actions Point to Heightened U.S. Efforts to Protect Imported Food Supplies

The U.S. enjoys the world's safest and most bountiful food supply. Securing our food and agriculture against intentional misdeeds is critical to our safety and economy and is becoming a key focus of the nation's homeland security efforts. This article briefly summarizes U.S. food safety law and reviews recent developments in food safety that affect growers, processors, distributors, importers and consumers of food products.

U.S. food safety laws traditionally have focused on protecting the nation's food supply from natural and accidental animal, plant and food pathogens. Since the events of September 2001, concern has arisen that pathogens or chemicals could be intentionally introduced and spread rapidly and easily through the food chain. Recent incidences of bovine spongiform encephalopathy ("BSE" or "Mad Cow") in a dairy cow in Washington State (from a farm in Canada) identified in a USDA surveillance program and the H7 strain of avian flu on two Delaware poultry farms have reminded us of the interdependence of our food sectors.

In his October 2001 executive order establishing the Office of Homeland Security, the President added agriculture and food industries to the list of critical infrastructure sectors needing protection. The Homeland Security Act of 2002 requires federal agencies to take steps to assure the continued safety of food and agriculture. Most recently, on January 30, 2004, the President issued Homeland Security Directive No. 9: Defense of United States Agriculture and Food. The President's directive "establishes a national policy to defend the agriculture and food system against terrorist attacks, major disasters, and other emergencies."

This article reviews four areas of recent activity focusing on the protection of imported food products:

- The November 2003 food security assessment of the Government Accounting Office ("GAO");
- The Food and Drug Administration's (FDA) implementation of the Bioterrorism Act and other initiatives;
- Recent food security initiatives of the Department of Agriculture; and
- Homeland Security Presidential Directive No. 9.

GAO on Food Security

On November 19, 2003, Lawrence Dyckman, a Director of GAO's Natural Resources and Environment team, issued a Statement for the Record before the Senate Governmental Affairs Committee, U.S. Senate entitled: "Bioterrorism: A Threat to Agriculture and the Food Supply." GAO reported that if they wanted to cause economic dislocation terrorists would target crops and livestock; and if they wanted to cause human injury they would target finished food products.

GAO's Statement summarized four of its recent reports recommending that FDA and USDA strengthen import and border food and agriculture inspection programs. GAO concluded that "[t]he U.S. agriculture and food sectors have features that make them vulnerable to bioterrorism attacks." GAO reports observed that U.S. Customs, USDA and FDA border and import inspection programs faced challenges in detecting

foot-and-mouth disease and BSE, given the volume of imported food and agriculture products. The U.S. imported about 125 million pounds of beef (0.35 percent of total imported) and about 1,000 cattle (0.003 percent of total imported) from countries that later discovered BSE, during the period when BSE would have been incubating. GAO documented security lapses at USDA's Plum Island Animal Disease Center, which studies serious animal diseases, including some that can cause illness and death in humans. Land, buildings and other facilities of the Plum Island Animal Disease Center were transferred to the Department of Homeland Security in June 2003.

GAO reported that the U.S. agriculture and food industries have largely been free of deliberate acts of contamination. In 1975, 750 people became ill when a group poisoned salad bars at several Oregon restaurants with Salmonella bacteria. In January 2003, 92 persons became ill after purchasing ground beef from a Michigan supermarket that was intentionally contaminated with nicotine.

A recent outbreak of foot-and-mouth disease caused the United Kingdom economy \$10 billion; a similar outbreak in the U.S. might cost the U.S. economy \$24 billion, spreading to one-third of the nation's cattle herds. GAO's report noted that both FDA and USDA had issued recommendations for securing food processing plants but that both agencies lack statutory authority to mandate security measures.

FDA's Implementation of the Bioterrorism Act

On June 12, 2002, President Bush signed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 ("the Bioterrorism Act"). Four provisions in Title III, Subtitle A, of the Act require the Secretary of Health and Human Services, through FDA, to propose and issue final food regulations: Section 303: administrative detention; Section 305: the registration of food and animal feed facilities; Section 306: the establishment and maintenance of records; and Section 307: prior notice of imported food shipments.

Registration of Food Facilities

On October 8, 2003, FDA announced the implementation of regulations requiring the registration of food facilities. Domestic and foreign food facilities that manufacture, process, pack or hold food for human or animal consumption in the United States were required to register with FDA by December 12, 2003. FDA will have for the first time an official roster of foreign and domestic food facilities, allowing timely notification and response in the event of a food safety threat. Exempt from notification are farms, private residences, transport vehicles, restaurants, retail food establishments, nonprofit food establishments, fishing vessels, and establishments that are entirely regulated by USDA. If an unregistered foreign facility attempts to import food into the United States, the food will be held at the port of entry unless FDA or U.S. Customs directs otherwise. Foreign food establishments must identify a U.S. agent.

Notice of Import

FDA's import notice regulations require food importers to provide the FDA with advance notice of human and animal food shipments imported or offered for import on or after December 12, 2003. This allows FDA to know, in advance, when specific food shipments will arrive at U.S. ports and what the shipments will contain. This advance information will allow the FDA, working with U.S. Customs and Border Protection, to more effectively target inspections and ensure the safety of imported

foods. The FDA expects to receive about 25,000 notifications about incoming shipments each day.

Detention

On May 9, 2003, FDA also proposed regulations implementing the provisions in the Bioterrorism Act that gave FDA the authority to detain any article of food for which there is credible evidence or information that the article poses a threat of serious adverse health consequences or death to humans or animals. The administrative detention authority granted to FDA under the Bioterrorism Act is self-executing and currently in effect.

Record Keeping

FDA also published on May 9, 2003, a proposed regulation implementing the provisions in the Bioterrorism Act that would require manufacturers, processors, packers, transporters, distributors, receivers, holders, and importers of food to keep records identifying the immediate previous source from which they receive food, as well as the immediate subsequent recipient to whom they sent food.

Other FDA Food Security Initiatives

Increased Food Import Inspections

Since 2001, FDA has quintupled the number of food import examinations. By 2002, FDA had more than doubled its presence to 90 ports of entry, and by July 2003, FDA had conducted over 62,000 food exams. The Technical Support Working Group (TSWG) of the Department of Defense and FDA are working with Sensor Research and Development to develop a prototype of a food pathogen detector. FDA is collaborating with the TSWG on a project at the John A. Volpe National Transportation Systems Center on a project related to the security of domestic and overseas transport of food.

Emergency Preparedness

FDA has established an Office of Crisis Management (OCM) to coordinate the emergency response activities of the five FDA Centers. In May 2003, FDA participated in the TOPOFF 2 terrorism exercise that simulated two separate terrorist acts including the possibility of food contamination by radiation. FDA has entered into an Inter Agency Agreement (IAG) with the U.S. Army to design and develop two mobile laboratories to be deployed at borders, ports, or other locations, to analyze import samples.

U.S. Department of Agriculture

Shortly after September 11, USDA formed a Homeland Security Council to coordinate the Department's efforts to secure the nation's agriculture against intentional acts. The mission of the Department's Food Animal and Plant Health Inspection Service (APHIS) is to protect plant and animal health to ensure a safe food supply. In 2003, APHIS border functions were transferred to the new Department of Homeland Security and approximately 2,600 members of the Department's border inspection service were transferred to DHS.

USDA has initiated numerous programs to guard against the accidental and

intentional introduction of foreign animal diseases and plant pathogens. The Department provided \$43 million to states, universities and tribal lands to increase homeland security prevention, detection and response efforts. As well, the Department is spending \$18 million to develop rapid tests for agents that pose the most serious threat to agriculture, including foot and mouth disease, rinderpest and wheat rust. The Department established an Office of Food Security and Emergency Preparedness.

Presidential Directive 9: Defending U.S. Food and Agriculture

On January 30, 2004, President Bush released Homeland Security Presidential Directive 9, which establishes a national policy to defend the agriculture and food systems against attacks, major disasters, and other emergencies. Directive priorities include increased monitoring and surveillance of food and agriculture, expanded vulnerability assessments of the food and agriculture sectors, the development of mitigation strategies to protect vulnerable food and agriculture sectors, as well as response planning and recovery and the expansion of food and agricultural security programs in the university community. Several executive agencies must quickly develop responsive programs. The Directive requires the Secretary of Agriculture within 120 days to make recommendations to the Homeland Security Council on financial risk management tools to encourage self-protection for food and agriculture enterprises vulnerable to losses due to terrorism. The food and agriculture industries may wish to consider the adoption of programs modeled on the SAFETY Act.

The SAFETY Act ("Support Anti-Terrorism by Fostering Effective Technology") may serve as a safe harbor for food and agricultural companies to insulate themselves from the liability that might arise out of a malicious act designed to compromise our food supply. Passed as part of the Homeland Security Act of 2002, this piece of tort legislation offers a variety of legal protections to qualified sellers, vendors, subcontractors and buyers of protective technology products and services. The key element of the SAFETY Act is that it provides protection for not only the manufacturers, suppliers and providers of security products and services, but also for possible targets that will need to employ such products and services.

Under the SAFETY Act, if a certified product or service fails, all vendors and buyers of the product or service are immune from liability. Only the manufacturer can be held liable; however, the manufacturer of a certified product is entitled to a presumption of dismissal. Food-related companies may benefit from the SAFETY Act and failing to take advantage of the Act's safeguards could have material adverse consequences, whether that means seeking to certify eligible products or services or seeking to purchase products or services that have been approved under the SAFETY Act by the Department of Homeland Security.

John D. Conner, Jr.
Washington, DC

■ Contact Us

If you would like more information about MLA's [International Law Practice](#), please contact any of the McKenna Long & Aldridge attorneys with whom you regularly work. You may also contact:

Allen B. Green
202.496.7523

Gordon D. Giffin
404.527.4020
202.496.7156

[↗ Back to top](#)

■ [About Us](#)

■ [Subscription Info](#)

McKenna Long & Aldridge LLP is a full-service law firm of approximately 375 lawyers and public policy advisors. Its [International Practice](#) provides business solutions in areas such as European Business & Regulatory Law, Arbitration & Litigation, Government Contracts, Intellectual Property, Trade, and Transactions, Tax & Investments.

If you would like others to receive future mailings of the International Law Report, please email their contact information to us at information@mckennalong.com

If you would like to be removed from our International Law Report mailing list, please email information@mckennalong.com

*This **International Law Report** is for informational purposes only and does not constitute specific legal advice or opinions. Such advice and opinions are provided by the firm only upon engagement with respect to specific factual situations. This message is intended as a transactional message for clients of the Firm. If you are not a client of the Firm, you have received it for informational purposes only and should not consider it an advertisement or solicitation.

• Atlanta • Brussels • Denver • Los Angeles • Philadelphia • San Diego • San Francisco • Washington D.C.

© Copyright 2004, [McKenna Long & Aldridge LLP](#), 1900 K Street, NW, Washington DC, 20006