

October 15, 2004

U.S. Ports—Still Vulnerable

Security of ports and shipping containers vital to nation's defense, economy

Last month, a judge in Yemen sentenced two men to death and four others to prison for their roles in the October 12, 2000, attack against the USS Cole in a Yemeni port. This sentencing should serve as a reminder of the risks faced by U.S. interests in ports at home and abroad. Causing the deaths of 17 U.S. sailors, the USS Cole bombing offered a small-scale example of havoc al Qaeda could wreak through an attack targeting the U.S. port system.

More than 80 percent of world trade travels by sea, with much of it passing through 361 U.S. commercial seaports. The sheer size and diversity of the nation's port system contributes to a steady flow of goods into and out of the U.S. economy, while also creating an attractive target for terrorists. The constant stream of traffic—ships, people, cargo—presents a wide range of potential security threats. The more than eight million cargo containers that arrive each year in U.S. ports are particularly vulnerable. Nuclear weapons, bomb components, even suicide bombers with provisions in hidden compartments, all could be shipped into the United States via containers. U.S. arrest and seizure records reveal that criminals have smuggled human beings, small arms, multi-ton shipments of narcotics and countless other forms of contraband in containers. A system so obviously accessible to criminal activity presents a viable means of terrorist attack.

A delicate balance must be struck between implementing tighter security and maintaining trade activity vital to the global economy. Despite passage of the Maritime Transportation Security Act (MTSA) of 2002 and the adoption of the International Ship and Port Facility Security (ISPS) Code, which mandated new security measures effective July 1, 2004, gaping vulnerabilities in port and shipping security still exist. The public and private sectors must share responsibility for enhancing awareness of and attention to the security risks inherent in the open U.S. port system.

This issue of The Lipman Report tracks the progress made in securing U.S. ports and cargo under the MTSA and ISPS, offering recommendations for the private sector to help strengthen port security.

Gaping vulnerabilities

The horrific tragedy of September 11, 2001, demonstrated that terrorists possess the ability

and means to strike effectively against the U.S. critical infrastructure. While the use of airliners in the attack resulted in immediate implementation of new security measures for commercial air travel, other equally vulnerable methods of transportation did not receive the same intense focus. The March 2004 commuter train bombing in Madrid, Spain, briefly focused attention on U.S. rail systems, but the nation's port system has not attracted widespread national concern.

An addendum to the report by the September 11 commission, which investigated what security failings contributed to the terrorist attacks, advised the Transportation Security Administration to develop a final plan by February 1, 2005, to protect passengers, equipment and facilities in all forms of transportation. The commission's recommendations include pre-board checking of cruise ship passenger names against terrorist watch lists and recovery plans to restart key transportation systems—including ports—in the event of a terrorist act.

The sheer volume of material entering U.S. ports makes it virtually impossible to inspect all containers using current methods, without causing a backlog that would significantly impede trade flow and negatively impact the world economy. Of approximately 15 million shipping containers, less than two percent are checked. These containers travel daily through the world trade infrastructure, posing potential security risks.

Experts continue to issue warnings about possible scenarios in which terrorists could exploit vulnerabilities in shipping containers to U.S. destinations. Dr. Stephen E. Flynn, author of *America the Vulnerable: How Our Government Is Failing to Protect Us from Terrorism*, has frequently voiced concern about the possibility of terrorists smuggling a weapon of mass destruction, including a nuclear bomb or components of a "dirty bomb," undetected in shipping containers. After arriving in the United States, compromised containers

(continued on next page)

U.S. Ports—Still Vulnerable

Security of ports and shipping containers vital to nation's defense, economy

(continued from preceding page)

could carry a bomb deep into the nation's interior by truck or by train.

Cargo containers represent a significant risk. Just one unchecked box carrying a bomb could produce massive losses. These containers must be secured in three ways: by ensuring that only legitimate goods are loaded, by preventing boxes from being intercepted and compromised en route, and by quickly and effectively inspecting any containers that arouse concern at any port.

Experts estimate that the possibility of detecting a weapon in a container from an untrusted source subject to inspection is less than 10 percent. Even if inspectors target a container and scan it, the probability of detecting a shielded nuclear weapon remains low due to potential obstruction from other cargo within the container. Prior to September 11, 2001, none of the major seaports, including New York, had X-ray or gamma-ray scanners in ports. While the use of such equipment is being implemented, time and money prevent immediate rectification of the problem. Development of a robust means for assuring container security should be a leading priority for government and business in post-9/11 security plans.

Should a bomb be activated within a shipping container in port, the attack would produce devastating consequences, not only in loss of life and destruction of the surrounding area, but also in terms of economic gridlock. All U.S. ports would likely be shut down, which would impact the global trade system, leaving retail shelves bare and assembly lines idle. A failed attempt to attack a port could still achieve terrorist goals of causing economic disruption. While loss of life and destruction of property might be averted, the process of closing a port to search for or disarm a bomb would produce significant delays in the delivery of goods, costing manufacturers, retailers, shippers and consumers time and money.

Slow progress

In response to the September 11 attacks, steps taken to increase port security without halting trade included the 24-hour rule, the Container Security Initiative (CSI), the Customs-Trade Partnership Against Terrorism (C-TPAT) and the creation of a National Targeting Center, which houses an Automated Targeting System.

Currently, all cargo or passenger ships entering U.S. ports must provide detailed information about crew, cargo and ship four days in advance of arrival. Under the 24-hour rule, the Bureau of Customs and Border Protection (CBP) requires mandatory manifest information to be submitted electronically 24 hours before cargo is loaded at foreign seaports bound for the United States.

Cooperation from 20 countries that are U.S. trading partners resulted in the Container Security Initiative, currently in effect at 26 ports, allowing for inspection of containers deemed "high risk" prior to being loaded on vessels destined for the United States. These inspections involve X-ray or gamma-ray scanners and radiation portals. Using pre-arrival information and input from the intelligence community, the Automated Targeting System evaluates containers for terrorist risk before cargo is loaded and shipped to U.S. seaports.

In partnership with the private sector, the CBP offers rapid processing of goods through U.S. ports in exchange for increased security efforts on the part of 7,000 companies enrolled in C-TPAT worldwide. These participants in global trade have provided assurances to CBP that they will take steps to improve security throughout their supply chains.

Scientists and engineers continue to search for methods of improving the cost and effectiveness of these and other security measures. One idea under development involves tiny sensors that can track the transit of a cargo container and monitor its integrity in the face of possible tam-

pering. The goal is to produce sensors that are cheap, small, global and reliable, with very low false alarm rates.

Many programs initiated by the United States have garnered support and cooperation from other countries, and international efforts to improve port security have also been implemented. In preparation for the 2004 Olympic Games in Greece, the United States loaned the host country two large-scale X-ray machines to scan incoming and outgoing cargo at a key port. The International Maritime Organization of the United Nations developed the ISPS Code, a set of security measures that calls for participating governments, companies and shipboard personnel to assess potential threats and implement appropriate security measures for each ship and port.

The U.S. equivalent to the ISPS, the MTSA mandates that port facilities and vessels conduct vulnerability assessments and develop security plans. Areas specifically addressed include passenger, baggage and vehicle screening procedures, security patrols, access control, and installation of surveillance equipment, as well as risk assessments and prioritization. The requirements affect an estimated 9,500 vessels, 3,200 facilities and 40 off-shore oil or natural gas rigs. The Coast Guard plays the primary role in overseeing the adoption of MTSA regulations to ensure uniform standards of security throughout the nation's port system. Ships that have not complied with these guidelines, or that have recently visited non-complying ports, can be turned away from U.S. shores, effectively barring nations from trading with the United States.

In evaluating progress made to protect the nation's ports, however, the assessment should focus not just on improvements since September 11, 2001, but on whether vulnerabilities that could be exploited by terrorists still persist. More than \$105 million has been earmarked for grants available to ports seeking implementation of additional security measures in Fiscal Year 2005,

but a bill to double port security spending on the development of equipment to detect nuclear weapons in containers was halted in the U.S. Senate. Increased funding will be required on the part of the government and the private sector to raise port security to the necessary level.

Responsibilities of private sector

The goals of the U.S. transportation system are to be as open as possible, as effective as possible, as reliable as possible and as low-cost as possible. In light of the speed with which business is conducted in the global marketplace, security has historically been viewed as an inhibitor that restricts access to the system, raises costs and undermines effectiveness and reliability.

Because 85 percent of the U.S. infrastructure is in private hands, the private sector must take action to implement incentives for investing in security initiatives. Nonetheless, recent surveys document that business leaders are not placing a high priority on security measures. The United States cannot afford to wait for another September 11 scenario before shoring up existing security risks. The private sector should demonstrate a unified front by taking proactive measures to improve national security.

Take a layered approach to security. Flynn advocates the need to develop creative security solutions that permeate the U.S. infrastructure. He notes that five "60% solutions" integrated into a unified security plan can cost less than a single "80 or 90% solution." Since terrorists will seek the easiest method of attack, the combined effectiveness of numerous security measures can avert potential disaster. A single security solution may be more costly and could possibly be circumvented, while several smaller steps may not only be less expensive, but may also provide more comprehensive security. Ensuring perimeter security around loading docks, for example, can reduce the risk of tampering with containers.

(continued on next page)

U.S. Ports—Still Vulnerable

Security of ports and shipping containers vital to nation's defense, economy

(continued from preceding page)

Security steps designed to deter the risk of terrorism can also reduce the risk of more common problems, such as illegal immigration, smuggling and cargo theft.

Develop security standards to ensure integrity of cargo at every point along the supply chain.

Effective security requires a shared effort among suppliers, transporters, manufacturers, sellers and users to develop and implement cohesive measures. Close collaboration among these entities can help to ensure that security programs minimize vulnerabilities, while maintaining an open, efficient flow of goods through the supply chain. Such all-encompassing solutions will require cooperation among global trading partners. These efforts should not only address ways to verify container security at all points of transportation, but also to develop plans for ensuring continuity, such as using alternative routes and suppliers, in the event of potential trade disruptions.

Establish public-private partnerships. The public and private sectors must work together to identify vulnerabilities, create standards and enforce policies so that everyone shares the cost and responsibility for the effort and no market advantage exists for leaving security problems exposed. For example, companies can spend \$50 per container to import merchandise in a "smart" container that includes a tracking device and intrusion alarm, enabling a thorough scanning before being loaded on a ship bound for the United States. If only one company or port invests in such practices, however, its profitability is undermined while security vulnerabilities simply shift to another shipment or location. By requiring universal standards, all companies will invest in the same security measures, enhancing the system's safety while not unfairly placing the financial burden on any one organization.

Acknowledge vulnerabilities, and avoid complacency. Both government and business must heed the warnings of security experts and recognize

that vulnerabilities still exist within the U.S. critical infrastructure. Once identified, these security risks require a comprehensive, unified plan of action. Companies should seek advice from local police, firefighters and other emergency responders to develop sound crisis response plans. In addition, educational campaigns by government agencies, local authorities and businesses can help the general public understand the risks still faced by the nation and the importance of investing in security measures.

Prior to September 11, 2001, the United States demonstrated little concern toward contents of nearly 20,000 containers arriving daily in U.S. seaports, until the cargo arrived on U.S. territory. Today, U.S. inspectors are stationed in international ports of trade, and the nation's allies have joined efforts to ensure that potential terrorist threats are not shipped under the guise of marketable goods. Despite this progress, experts warn that much more needs to be done to secure the nation's ports—and the economy.

While no single solution exists, the private sector can implement measures to enhance port security. Businesses and the public cannot rely solely on government regulations or self-imposed industry guidelines to protect the nation's ports from an attack of the magnitude of September 11, 2001. Each individual and organization holds responsibility for homeland security efforts, including protection of all aspects of the nation's transportation system. Awareness, education and basic security procedures must continue to improve, so the terrible tragedy that tarnished U.S. air travel cannot recreate horror through the nation's trade system, achieving the terrorists' goal of economic destruction.



The Lipman Report Editors