

January 15, 2003

## Vulnerability of Ports Endangers United States

### Safeguarding harbors necessary to prevent terrorist attack, economic disaster

*In the rush to strengthen airport security following the September 11, 2001, attacks, weaknesses in U.S. seaport security have received significantly less attention in terms of legislative and financial support. This oversight cannot continue. The catastrophic terror attacks of September 11, 2001, demonstrate that anything can happen in the new war against the United States. The nation cannot necessarily rely on history to determine how or where the enemy will strike next. Consequently, the public and private sectors must consider all potential vulnerabilities when assessing risk and developing appropriate security measures.*

*Many characteristics of seaports make them inherently susceptible to terrorist attack: their size, open accessibility by land and sea, location in metropolitan areas, and ready transportation links to key sites within U.S. borders. Naturally, all of these traits contribute to the effectiveness of ports at directing the flow of goods in and out of the nation, and a terrorist organization can easily exploit these vulnerabilities. The challenge lies in tightening security procedures without clogging the flow of trade and disrupting the global economy.*

*This issue of The Lipman Report examines the current state of port security and the measures taken since September 2001, and offers recommendations on how private businesses can contribute to this critical aspect of the homeland security effort.*

#### **Porous security**

International commerce relies heavily on the efficient operation of U.S. seaports, through which more than six million containers enter the nation's borders each year. More than 95 percent of non-North American foreign trade arrives by ship; for certain commodities, such as foreign oil, that figure increases to 100 percent. The sheer volume of material entering U.S. ports makes it physically impossible using present methods to significantly increase the percentage of containers inspected without creating a negative domino effect throughout the world economy. Taking advantage of this situation, drugs and illegal aliens routinely enter the United States, often hidden among legitimate cargo. The idea that terrorists or any other enemy might also use these avenues to

introduce a nuclear weapon, for instance, is not far-fetched in the post-September 11 world.

Further complicating the situation is the fact that many of the country's port facilities are formed by extensive networks involving multiple jurisdictions and both public and private interests. The federal government holds jurisdiction over harbors and interstate and international commerce, while state and local governments have the primary responsibility for port regulation. Additionally, many of the enterprises at seaport complexes lie in private hands; more than 150 plants make up the industrial complex at the Port of Houston. While the U.S. government is tasked with the overall mission of homeland security, the variety of interests in the national port system demands intimate cooperation of all entities involved for the development and implementation of an effective security strategy. Only by addressing the multipronged nature of responsibility for port security can the players involved expect to reach a solution that safeguards both security and economic interests.

#### **Drastic consequences**

A terrorist strike against U.S. ports need not come to fruition for it to impact the nation's business. Even without the loss of life and destruction that an explosion could bring, for example, closing a port to search for or disarm a bomb would produce an infinite chain reaction. The potential economic ramifications can be seen in previous port strikes.

When a 10-day labor lockout affected 28 ports on the West Coast just months ago, analysts estimated that the closure cost the country between one billion and two billion dollars per day. The dispute between longshoremen and managers had worldwide consequences: farmers could not ship perishable goods overseas, automotive plants shut down because they could not receive parts and local merchants from Seattle to San Diego felt the pinch as they failed to meet consumer needs.

(continued on next page)

---

## Vulnerability of Ports Endangers United States

Safeguarding harbors necessary to prevent terrorist attack, economic disaster

(continued from preceding page)

Once President George W. Bush intervened and the ports reopened, the backlog of shipments meant that retailers encountered delays in receiving holiday shipments and overseas exporters waited for up to 10 weeks before their products were unloaded. In 1997, when 11 harbor pilots went on strike in Los Angeles, the nation's second-busiest port came to a virtual standstill, causing the port alone to lose nearly half a million dollars daily. Such an interruption created by more ominous circumstances could create even greater disruption in the U.S. economic system and beyond.

Last fall, a Washington, D.C.-based think tank partnered with a global management consulting firm to conduct a two-day port security wargame. In the exercise, two radioactive dirty bombs entered the United States on the same day: one by ship, which went undetected until it fell off a truck in the port complex, and the other by truck over the Canadian border, unpacked from a shipping container in the Midwest. Meanwhile, port authority police in Georgia arrested three men, one on an FBI watch list of suspected terrorists, on suspicion of attempted cargo theft. The decisions made by the stakeholder teams—representing federal policy-makers, carriers, border operations, commercial businesses, port authorities and a control group—produced drastic consequences: Every port in the nation was shut down for eight days, producing a backlog of deliveries that required more than three months to resolve. The resulting loss of revenue to the U.S. economy was estimated at \$58 billion.

### Current progress

Several federal agencies, including the U.S. Coast Guard, the Customs Service, and the Immigration and Naturalization Service (INS), have been particularly active in upgrading security at the nation's seaports.

Immediately following the September 11 attacks, for example, the Coast Guard recalled all cutters assigned on routine patrols for drug and immi-

gration enforcement and repositioned them at entrances to the nation's more strategic ports, including Boston, Los Angeles, Miami, New York and San Francisco. Many of these vessels have since returned to other tasks, although several remain assigned to national security. The agency has also started conducting initial risk assessments of ports, aimed at identifying high-risk areas to improve the effectiveness of harbor patrols. Other Coast Guard initiatives include increasing the surveillance of passenger ships and other high-interest vessels, such as naval ships and petroleum tankers, and working through the International Maritime Organization to strengthen maritime security worldwide.

Likewise, the U.S. Customs Service is developing programs to improve cargo prescreening and container inspection, and the INS is in the process of creating an entry and exit system that will create records for aliens arriving in the United States and match them with those individuals' departure records.

Several state agencies have also taken up the call to increase security at the nation's seaports. Florida, for instance, has been an early leader in this effort—even before the September 11 attacks. In 2001, that state became the first to establish security standards for ports within its jurisdiction and to require those ports to maintain security programs that comply with those standards. The Port of Tampa, the largest port in Florida, has already conducted background checks on and issued new security credentials to 5,000 employees, and is currently working its way through the remaining 2,000 workers.

In another example, plans are underway to transform the adjacent ports of Los Angeles and Long Beach into a testing ground for new security devices and strategies aimed to thwart terrorist attacks. Proposed enhancements include the following:

- A \$40-million inspection center at Terminal Island for the analysis of suspicious cargo;

- A 40,000-square-foot headquarters for the Los Angeles Port Police, with video camera surveillance of activities between the Vincent Thomas Bridge and the breakwater; and
- A \$35-million credential system that incorporates sophisticated identification cards for port employees, containing a holographic photo and the signature of the worker, as well as his or her fingerprints, driver's license number and criminal background.

The experiment will also test new tamper-proof locks and other security technology, including radiation detectors that can identify a nuclear bomb hidden in a container on a train moving at 30 miles per hour.

#### **Further action needed**

As in many other aspects of homeland security, the United States has made significant progress in tightening the security of its seaports during the past year, but much work remains for both the public and the private sectors.

The federal government has made additional funding available for enhanced port security, but a more substantial investment is required. As part of a Department of Defense supplemental budget appropriation for fiscal year 2002, the Congress designated \$93.3 million for port security grants, and subsequent legislation last fall augmented this amount by \$125 million. However, as seen by the proposed improvements for Los Angeles and Long Beach, port security measures can be quite costly. The Port of Tampa, for instance, has received \$2.9 million in state funds and \$3.5 million from the federal government to increase security, but estimates that it needs an additional \$24 million to complete its security upgrades—excluding a projected \$5 million per year for new security personnel. Private organizations with port operations need to help supplement federal appropriations for additional security measures—even if only in the interest of self-preservation. After

all, disruptions at a seaport can have potentially disastrous consequences on those organizations relying on just-in-time delivery of merchandise. Security needs are great, and funds are limited.

To begin, each seaport needs a thorough assessment of its facilities to identify potential security threats and develop appropriate countermeasures. After September 2001, the U.S. Coast Guard started a process to survey 55 of the nation's 361 ports during a three-year period—an important step that must be extended throughout the system. This analysis should start with a preliminary assessment: compilation of a physical description of the port's layout and essential utility services, and a listing of all personnel and agencies involved in securing the facilities. Next, an on-site assessment will evaluate existing security procedures and related equipment, focusing on the following areas: access control procedures; security force deployment and management; inspection, control, surveillance and security of cargo and baggage; internal auditing practices for security equipment and keys; protective lighting, intrusion detection devices and communication systems; and emergency response equipment and procedures. Finally, the inspection team must address vulnerabilities uncovered during the assessment and offer practical solutions that will increase security without overly impeding port operations.

While a risk assessment will help identify weaknesses at specific facilities, the following recommendations address broader issues in the need to tighten the nation's seaports:

- **Strengthen public-private partnerships.** An incident requiring a port closure quickly creates problems for businesses and consumers, making cooperation between the government and corporations critical. Because many port facilities rest in private hands, the security program for each port needs to be developed as a joint effort. Such collaboration will help ensure that the program minimizes risk, while

(continued on next page)

## Vulnerability of Ports Endangers United States

Safeguarding harbors necessary to prevent terrorist attack, economic disaster

(continued from preceding page)

maintaining an open, efficient flow of goods through the supply chain. Furthermore, measures designed to fight the threat of terrorism will have the added benefit of deterring more common problems, such as illegal immigration, smuggling and cargo theft.

- **Begin security at the point of origin.** The overwhelming amount of cargo that enters the United States through its ports makes physical inspection practically impossible. Increasing the percentage of containers examined would produce extensive backlogs, adversely affecting the U.S. and global economies. Consequently, security must be strengthened throughout the system of delivering goods to market, from the manufacturers to every link in the transportation chain: land, rail, sea and air. This complex, but necessary process will require close cooperation with all global trading partners.
- **Develop security standards to ensure the integrity of cargo.** The engineers behind the intermodal revolution in transportation did not factor security into their designs; they focused on lower transport costs and greater speed and efficiency. To compensate for the difficulty of increasing cargo screening, the shipping industry needs to develop security standards at loading facilities. Compliance with these standards—verified through independent audits and certification—should be required for gaining access to international transportation terminals.
- **Build security into everyday processes.** Safeguarding this portion of the U.S. infrastructure demands a more comprehensive approach than simply trying to address vulnerabilities at arrival ports or at congested land borders. Every entity involved in port security needs to reassess its role in transporting items into and out of the United States and to examine how to incorporate security measures into daily activities. This

process should not only address ways to make standard business procedures safer, but also include options to ensure operational continuity in the event of a breach, such as alternative suppliers and transportation routes.

*Several developments in the last 18 months have brought the issue of port security to the forefront of national concern. Both the continuing campaign against terrorism and the threat of war with Iraq raise the danger of an attack capitalizing on vulnerabilities in this highly accessible and critical part of the U.S. infrastructure. The country's enemies have demonstrated a willingness to implement unconventional weapons against the United States, forcing the federal government and private businesses alike to consider all possibilities in safeguarding U.S. operations at home and abroad.*

*As seen in the catastrophic attacks of September 2001, the United States cannot rely on its position as the sole global superpower to deter domestic assaults. Port security, like aviation security, must be hardened against attacks aimed at the ultimate destruction of the American way of life. Given the economic ramifications of impeding the flow of cargo through the U.S. port system, this need presents enormous challenges and no simple solutions.*

*The integral role of private industry in the operation of U.S. seaports demands close cooperation between the federal government and corporate America. Even organizations not directly involved with the nation's ports will suffer dramatic repercussions if U.S. enemies succeed in stanching the flow of trade through these crucial arteries. At stake is nothing less than the continued viability of the global economy.*



The Lipman Report Editors