

October 15, 2005

Securing shipping containers in U.S. ports

Public and private sectors must collaborate to strengthen security of global supply chain

According to the U.S. Customs and Border Protection (CBP), nearly 9 million containers arrive in U.S. ports each year, representing an important cog in the wheels of commerce. These cargo units also represent a potential means by which terrorists could strike a devastating blow to the economic stability of the nation. Experts fear an inevitable attack using a "dirty bomb" (explosive devices containing radioactive material) or other weapon of mass destruction smuggled into the United States disguised as a legitimate import. Once on U.S. soil, the cargo container could transport its deadly contents anywhere in the country via rail or truck.

In an effort to reduce the risk of nefarious agents being delivered via cargo shipments to the world's ports, port officials in Hong Kong, the world's second-busiest port, are testing a prospective new program. Science Applications International Corp. of San Diego supplied the Hong Kong Terminal Operators Association with scanning machines that electronically scrutinize every container, hauled through the scanners on trucks. The first scanner checks for nuclear radiation, while the other uses gamma rays to seek out any dense, suspicious object made of steel or lead inside the containers that could shield a bomb from the nuclear detector.

To date, the U.S. Department of Homeland Security has not announced whether such a comprehensive program might be implemented at U.S. ports. This issue of The Lipman Report examines the risks posed by unexamined containers and measures that can help enhance security of the nation's shipments.

Existing threats to cargo containers

Since the terrorist attacks of September 11, 2001, U.S. government and law enforcement agencies have sought methods of improving the nation's security. The immediate focus on airline security resulted in more stringent screening of passengers and bags. Other transportation areas, however, did not receive the same attention despite experts warning that trains, subways, trucks and ships required enhanced security measures as well. After the train bombing in Madrid, Spain, in March 2004 and the subway and bus bombings in London, England, in July of this year, height-

ened awareness prompted new initiatives on other forms of passenger transportation.

While the protection of individuals in transit is vital, security for the nation's cargo containers must not be overlooked. About 90 percent of all world cargo moves by container, providing ample opportunity for terrorists to exploit a lack of scrutiny regarding their contents. Experts have 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.

A single unchecked cargo container transporting a bomb could produce devastating losses. However, a terrorist strike could wreak havoc without being carried out successfully. Even without the loss of life and destruction that an explosion could bring, closing a port to search for or disarm a bomb would create a domino effect. A backlog of containers waiting to be inspected would bring the flow of commerce to a halt as supplies and goods remained undelivered to businesses and the public. The reliance on "just-in-time" deliveries by manufacturers and retailers means that a disrupted supply chain would produce an almost immediate lapse in products available for public consumption. For example, a labor dispute in October 2002 led to a 10-day lockout of longshoremen on the West Coast and billions of dollars in losses for U.S. businesses.

In January 2002 the CBP, formerly U.S. Customs, announced the Container Security Initiative (CSI) to protect the global trading system by targeting containers that pose a potential threat. First implemented in worldwide ports that ship the greatest volume of containers to the United States, the initiative has continued to expand to strategic locations, currently in more than 35 ports around the world. Along with the CSI program, the Customs-Trade Partnership Against Terrorism (C-TPAT) was developed

(continued on next page)

Securing shipping containers in U.S. ports

Public and private sectors must collaborate to strengthen security of global supply chain

(continued from preceding page)

under the direction of soon-to-be-retired Customs Commissioner Robert C. Bonner in an effort to determine the contents of cargo containers before the shipments leave for the United States.

The C-TPAT is a voluntary reporting system that looks at the chain of supply for foreign goods. Recognizing that the highest level of cargo container security requires cooperation from businesses at every point in the supply chain, the CBP has sought participation in the security effort from importers, carriers, customs brokers, manufacturers and other entities.

Participants in the program provide assurances to CBP that they will take steps to improve security throughout their supply chains. The organizations must complete an application and conduct a comprehensive self-assessment of their security measures. In exchange for increased security efforts on the part of 7,000 private sector companies enrolled in C-TPAT worldwide, the CBP offers rapid processing of goods through U.S. ports. Verification of the participants' compliance with required security improvements, however, has been slow, resulting in a "trust, don't verify" system in many cases.

The CSI relies on intelligence gathering and the examination of cargo manifests to identify and target containers that pose a risk for terrorism, which are pre-screened at their port of departure. Officers deployed to participating ports cooperate with host nations to prevent shipping containers from being exploited by terrorists. Once these pre-screened containers reach the United States, they receive expedited processing upon arrival.

A recent report by the Government Accountability Office found that the container program had led to improved information sharing between U.S. and foreign customs officials and greater international cooperation. But in some cases, customs

has not been able to obtain permission from host governments to operate in overseas ports. Should a terrorist attack occur, those ports participating in CSI would also have a competitive advantage because they would experience less disruption with trade to the United States because of the pre-approved security measures already in place.

To supplement the security programs initiated by the CBP, new technologies, such as tamper-evident seals, are being tested. Radiation portal monitors have been deployed at seaports, land border points of entry, international airports and other locations to detect incoming goods, people and conveyances for radiation that could indicate nuclear materials, such as for a "dirty bomb." Hand-held radiation scanners were distributed by CBP to major U.S. ports, but the devices are used only on containers that have been deemed a high risk, as an alternative or a precursor to physical inspections.

At the CBP's National Targeting Center in Reston, Va., U.S. customs agents use the automated targeting system computer program to evaluate information provided by shipping agents to search for potential terrorist weapons among cargo. The system checks the information against government databases and identifies high-risk cargo, allowing authorities to determine if these containers should undergo scrutiny at the port of entry or overseas, or whether they should be barred from entering the United States. Through these efforts, the CBP strives to "examine cargo effectively without slowing the flow of trade."

Critics, however, say this method fails to provide the level of security necessary, noting that the information on shipping documents is often vague and intelligence from many locations may be unreliable. Currently, fewer than 6 percent of the containers destined for U.S. ports are deemed "high risk" by the U.S. Department of Homeland Security and pulled aside for exami-

nation by customs inspectors. The inspection program recently tested in Hong Kong offers a possible solution for raising the level of scrutiny devoted to shipping containers arriving in the United States.

New initiative overseas

As trucks in Hong Kong carry containers through two giant scanners, port operators review monitors displaying the results of the process. Images similar to X-ray results appear on the screen for each container and are recorded on a computer server, along with the tracking code on the side of each container. Proponents contend that this system improves the security of the global shipping network without unacceptably slowing the flow of commerce.

In addition to expanding the inspection process to all containers, this system saves critical information that could be used by customs officials and law enforcement in ports around the world to trace the origins of a container used in a terrorist attack or to help identify suspicious cargo en route to its destination. Should a container smuggling a weapon be discovered, the stored information could also help to prevent detrimental disruption of the global shipping system, allowing authorities to selectively stop ships transporting other containers from the same source or that had similar results from the scanning.

Since the program was implemented, more than 250,000 scans have been stored in Hong Kong, including many for containers shipped to U.S. ports. While the CBP has suggested that the system could play an important role in reducing the threat of terrorism, it has not indicated that a similar system would be used within the United States. Instead, the agency stands by the current security measures in place. While enforcing another layer of security would require a significant investment in time and money, experts have reported that if shippers picked up the cost of the Hong Kong project, it would cost an additional

\$6.50 a container, a fraction of the approximately \$1,900 to send a 20-foot container from Hong Kong to Los Angeles.

Businesses must take proactive steps

Increased layers of security regarding cargo containers not only reduce the risk of these items being used in a terrorist attack, but can also help protect against theft. A two-pound box of electronics known as an SC-tracker has recently been used to remotely monitor the path of shipping containers. The device has been hidden inside crates by shippers and trucking companies to track the movements of the shipments, and an FBI investigation following such a shipment recently resulted in the bust of a notorious theft ring. Enhancing authorities' ability to monitor cargo shipments can impede terrorist efforts in addition to stemming stolen merchandise that costs the retail industry between \$10 billion and \$15 billion annually. The FBI has disrupted thefts in which they believe the resold merchandise generated money for terrorist groups in the Middle East.

Measures by the U.S. government to improve security regarding ports and the containers shipped there must be supplemented at the state and local level. While federal grants continue to be issued, the funds cover a wide range of projects, producing inconsistencies along the national shipping supply chain. For example, a recently announced \$2.5 million grant for the Port of New York/New Jersey and the Port of Camden has been allocated for state police vessels capable of carrying underwater cameras to scan ship hulls and docks for explosives, as well as infrared cameras for nighttime surveillance. On the opposite coast, minimum-wage private security officers and a port police force of fewer than 100 represent the primary security for 7,500 acres of facilities along 49 miles of waterfront shared by Los Angeles and Long Beach. Since

(continued on next page)

Securing shipping containers in U.S. ports

Public and private sectors must collaborate to strengthen security of global supply chain

(continued from preceding page)

the 9/11 attacks, these two cities have received only \$40 million in federal grants to improve physical security—equivalent to the amount U.S. taxpayers spend daily on domestic airport security.

With the protection of the nation's critical infrastructure falling primarily to the private sector, businesses at every point in the global supply chain must join together and take steps to enhance security. The following measures can contribute to improved security for individual businesses as well as the nation.

Conduct risk assessments. Each seaport and participant in the global supply chain must embrace the U.S. Coast Guard Maritime Security (MarSec) requirements in conducting thorough assessments of its facilities to identify potential security threats and develop appropriate countermeasures. Such analysis should start with a preliminary assessment describing the port's physical layout and essential services. Evaluate existing security procedures and related equipment, focusing on 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. Address vulnerabilities uncovered during the assessment and offer practical solutions that will increase security without overly impeding port operations.

Implement layers of security. Rather than relying on a single program or security procedure, businesses and the government must implement several overlapping layers of security to reduce the risk of terrorists, who will likely seek a "soft target." A combination of measures such as patrolling loading docks to deter unauthorized access, ensuring perimeter security around

shipping containers, thoroughly examining manifests for suspicious information and tracking shipments from their point of origin to destination can reduce the risk of terrorism while also helping to prevent more common problems, such as illegal immigration and cargo theft.

Establish effective partnerships. An effective security plan for ports and shipping containers requires a collaborative effort among all industries involved in the supply chain. Shared steps for ensuring the security of containers at all points along the trade route should be developed, along with plans for ensuring continuity in the event of potential trade disruptions, such as using alternative routes and suppliers. In addition, the private sector must urge government agencies to adopt a more aggressive approach to port security, working together to identify vulnerabilities, create standards and enforce policies so that everyone shares the cost and responsibility.

While steps have been taken to improve cargo security at U.S. ports, experts warn that current procedures only cover a minuscule percentage of the massive numbers of containers arriving daily. Should terrorists take advantage of the glaring vulnerabilities that still exist, it could have a crippling effect on the national—and global—economy. A successful attack's ability to disrupt the transportation of goods would impact a broad spectrum of industries. As a result, businesses in the private sector must take steps to bolster security, rather than relying on the U.S. government to effectively protect against a dangerous delivery through the nation's ports.



The Lipman Report Editors