

## INDUSTRIAL MANAGEMENT & TECHNOLOGY

### Protecting America's Ports

The government is trying, critics say it's not doing enough, and importing already takes longer and costs more.

FORTUNE

Sunday, October 26, 2003

By Philip Siekman

A bit over a year ago, all the ports on the West Coast were shut for 11 days in a contract dispute with the International Longshore and Warehouse Union. That cut the flow of more than 60% of U.S. imports. Container ships piled up, retailers' shelves emptied, and factories waiting for foreign parts stalled. Cost to the U.S. economy: by one estimate, \$15.6 billion.

While that was happening, managers from importing companies and shipping lines as well as government officials were facing a scarier scenario in a war game devised by Booz Allen Hamilton: A cargo container carrying a dirty bomb, a conventional explosive wrapped in radioactive material, falls off a truck leaving the port of Los Angeles. Seaports and border crossings are shut down, and all foreign trade is halted for 12 days, staggering the U.S. economy and sending costly ripples around the globe. Booz's estimate of the probable hit to the U.S. economy: \$58 billion.

In the post-Sept. 11 world, the U.S. needs to secure the ports through which it annually imports nearly seven million containers holding \$500 billion worth of goods. It must ensure that none of those boxes contain material that is explosive, radioactive, or biologically malignant. That effort is underway, but it is an enormous task that some believe is nearly futile. Says James Carafano, a senior research fellow at the Heritage Foundation in Washington, D.C.: "The infrastructure is so huge, and the vulnerability is so massive. To protect it and inspect all the cargo would consume zillions of dollars."

The push to deal with terrorism and trade is handicapped by history. Systems developed to move goods globally were designed for efficiency, reliability, and speed, not security. Says Rear Admiral Larry Hereth, the Coast Guard's director of port security: "There were lots of regulations out there for safety and hazardous cargo, but almost nothing for security. We're starting from ground zero." Importers and container-ship operators understand that, but importing already takes longer and costs more because of changes imposed since Sept. 11. Companies worry that delays and expense will mount as the government experiments with schemes and high-tech equipment in its effort to deal with a seemingly unending list of questions starting "What if?"

Hereth says the government recognizes the danger and will step cautiously. "You have to be careful about security's impact on commerce," he says. "We don't want the bad guys to win by us choking our economy to death." But critics still complain that government officials tend to work everything out on their own without consulting the people who deal daily with international shipments.

Most big U.S. importers are making their own efforts to tighten security throughout their supply chain, but coping with terrorism would stretch their capabilities. DaimlerChrysler maintains a permanent crisis-control center at its U.S. headquarters in Auburn Hills, Mich. Home Depot mobilizes crisis teams on an as-needed basis and assembles them close to the affected area. Sears has a permanent operations center at its headquarters in Hoffman Estates, Ill., set up by Gus Pagonis, who's in charge of its logistics. As a three-star general, Pagonis did the same job in Desert Storm. But corporate crisis centers are meant to handle hurricanes, blizzards, and truck strikes. Responding to a terrorist act would be a lot more challenging. Says Pagonis: "Shutting down the ports? If that's what it takes, we have to live with it and suffer through it, and business will have to lose some money."

Any retailer importing products from Asia or manufacturer shipping parts to its American plant is already aware that its supply chain is being shaken by government efforts to make incoming cargo shipments less susceptible to ill use. Two years ago about 98% of containers were offloaded from ships and moved from ports with no more than an examination of documents. Today the percentage is down to around 94%.

Well-known firms with well-worn ruts in their trade routes are the least likely to be hurt when shipments are delayed on the container terminals. According to PIERS, the Port Import/Export Reporting Service, Wal-Mart, the busiest importer, brings in about 175,000 containers a year, while Home Depot and Target each import 100,000-plus. For them, a few boxes held in port is a small inconvenience.

Lesser-known companies importing 100 or so containers a month are more likely to be inspected—and more likely to suffer from delays. If one container on a bill of lading is pulled out, the others are also held up. Delivery dates are missed. Costs pile up. Terminals charge storage of some \$100 a day if the containers stay too long. U.S. Customs bills for time spent on inspections. If the inspection station isn't on the terminal, there's transportation to pay. John Wood, general manager of Garden Zone in North Charleston, S.C., which imports fencing and garden products from Asia, says one container inspection can cost him several thousand dollars.

The Department of Homeland Security has put together programs, regulations, pilot projects, and grants aimed at improving the security of seaports and ocean-borne cargo. But critics complain that its efforts don't live up to their billing. The U.S. General Accounting Office's comment about one program's "relatively immature state of governance and management" sums up what it says about most of them. U.S. Senator Fritz Hollings (D-South Carolina) says, "This administration still hasn't gotten serious about [port security]. The President continues to be long on rhetoric and photo ops, and short on substance and resources for our ports."

At the center of the DHS strategy is an effort to push security threats away from U.S. shores (see diagram). U.S. Customs inspectors are being stationed in foreign ports to work on risk assessment and to screen U.S.-bound cargo, a program known as the Container Security Initiative. Customs now has CSI agreements with 19 foreign ports that

together account for more than 60% of U.S.-bound containers. Some 16 ports—including Hong Kong, Singapore, and Bremerhaven, Germany—already have U.S. Customs agents on the ground. Arranging agreements is something of a diplomatic challenge. But foreign port authorities go along, since shipments from ports that aren't in the program are more likely to be delayed for inspection.

To get U.S. companies to police their own supply chains, Customs, now known officially as the Bureau of Customs and Border Protection, is dangling a carrot and holding a stick in the form of the Customs-Trade Partnership Against Terrorism, or C-TPAT (pronounced C-T Pat). Its goal is to beef up protection for, say, 75% of the arriving cargo, so that inspectors can spend their time looking more closely at the remaining 25%. Participants must warrant that they have a tight security plan in place along the full length of their supply chain. That could involve, for instance, attesting that a supplier in a remote Chinese village is loading its U.S.-bound containers inside a properly fenced or guarded facility and has performed background checks on the part-time laborers it has hired. Home Depot is doing that. To educate its many vendors, it sent teams to China that included people from the companies that handle its freight.

C-TPAT is a voluntary program, but the message is to "join up or risk inspection delays when your containers arrive in the U.S." Seven big companies—BP America, General Motors, Ford, DaimlerChrysler, Motorola, Sara Lee, and Target—signed up first to work with Customs to get the program going. Since early 2002 about 4,500 companies have indicated that they also plan to participate. About 2,000 have had their security plans approved by Customs. Some companies, such as electronics manufacturers Solectron and Flextronics, have started to make compliance with the C-TPAT requirements a clause in their purchasing contracts. Greg Stein, vice president of transportation for Flextronics, says that's become a criterion for selecting cargo carriers as well as suppliers.

Some argue that C-TPAT is flawed. They contend that Customs is assuming that terrorists won't be able to identify the containers that are most likely to pass through unhindered. They also point out that C-TPAT is only as good as the security plans of its members. As of September, Customs had checked up on just a little more than 100 companies to see that their plans had been implemented. Big companies will probably match action to word. But what about the thousands of others? George Weise, U.S. Customs Service commissioner from 1993 to 1997 and now an executive with Vastera in Dulles, Va., which provides global trade-management services, says companies frequently ask him, "What's the minimum I can do to get by?"

Shippers, particularly ocean carriers, have also been coping with a new Customs requirement that tightens regulations on paperwork. In the past shippers could drop off a container at a dock and say, "Just load it. I'll get you the paperwork later," even if "later" meant as the ship was tying up in the U.S. Now Customs wants complete documentation delivered in electronic form 24 hours before any cargo headed for the U.S. is loaded at the port of origin. John Hyde, U.S. director of security for Maersk Sealand, which hauls more containers to the U.S. than any other company, says the 24-hour rule has caused a "big regearing of our whole process." The consequences are real. If the shipper misses the

deadline, it misses the sailing. If the shipping line loads the cargo anyway, it pays a \$5,000 fine for the first offense and double that the next time.

The new rule also means that some foreign factories now take longer to deliver shipments to the ports. Sony says that complying with the 24-hour rule can add 24 hours to its supply chain by delaying shipments at the factory until all the documents are in order. Michelin, the French tiremaker, ships a huge range of finished tires into the U.S. from its plants in Europe and Asia. Its North American import-export manager, Stan Pech, says the rule initially caused "a lot of confusion" among its sister companies, which had to get better organized before sending products to the U.S. Mikasa, another French-owned company, had a bigger problem. One of the world's biggest marketers of dinnerware and crystal, Mikasa buys everything from third parties. It had to persuade managers of some 200 factories in 40 countries to comply with the requirement.

A gap remains between what the government hopes to achieve and the effectiveness of its actions. DHS officials contend that "all high-risk cargo" arriving in the U.S. is now being inspected. But that means that Customs inspects boxes about which it has questions, not that it spots everything questionable. Since October 2001 the bureau has been operating an "automatic targeting system" at a center in Washington's Virginia suburbs where it assembles shipping documents and intelligence data from various sources to evaluate inbound cargo. Outsiders wonder whether the targeting is effective. For good reason, nobody knows what gets Customs' attention, other than the obvious—a suspect shipper or consignee, something odd about the documents, or a concern about the vessel's last port of call.

Once cargo is onshore and singled out for attention, the quickest inspections are done by VACIS devices—one of those acronyms for which even users can't remember the full name: Vehicle and Cargo Inspection System. The machine uses a cobalt-60 source to generate gamma rays from a projector to create a CRT image of a container's contents. The image is a bit coarser than an X-ray but is still readable, won't zap a stowaway, and is relatively fast. Customs officers take about two minutes to scan each container and another two to five minutes to examine the image. A VACIS machine can process about 100 containers during a 12-hour shift.

About three out of four containers are released after they roll past the VACIS. The remainder are opened for complete examination. That can mean taking out everything inside, looking it over, and then stuffing it back in the box. If the cargo is not loaded on pallets, the inspection can take hours. Toto, a Japanese maker of toilets and other bathroom fixtures, imports about 150 containers a month and can pack upwards of 1,300 toilet tanks in a 40-foot container. Customs has never had a problem with Toto, but its experience with drug smuggling makes it uneasy about loads with so many potential hiding places. If Customs decides to inspect one of those containers, Toto is likely to not see it for a week.

Customs has put VACIS in the major ports as well as at Canadian border crossings; additional ones are on order at about \$1 million each. But it is still doing little more than

sampling shipments rather than checking every box. To make sure it doesn't miss anything, DHS is looking for a technological rescue. It's experimenting with other inspection systems, including machines that scan containers for radiation. It is also being inundated with ideas for electronic devices that will turn dumb steel boxes into "smart" containers. Those ideas, which include electronic seals and global positioning satellite readers, make shipping lines and other container owners uneasy. Something like 10.8 million containers travel the world's trade routes, and almost any one of them could end up in the U.S. at some point. Adding a self-powered gadget of questionable reliability to every container might cost more than it's worth.

Two approaches hold promise. Given the right opportunity, smugglers can remove and then replace the doors on a container at the hinge points without disturbing the seal on the bars that latch them shut. Maersk, for one, is starting to use containers on which the doors jam if somebody tries to remove the hinges. Other companies, including Savi Technology in Sunnyvale, Calif., are pushing RFID—radio-frequency identification—in the form of labels that electronically store information, such as origin, content, and shipper, that can be retrieved by an electronic reader. Big retailers and the Department of Defense are moving to wholesale adoption of RFID labels, which should help solve technical problems and drive down costs.

Some container owners say that putting information on a box that can be retrieved by anybody with a reader will help thieves spot ones worth pilfering. But William McLean, head of operations at the South Carolina State Ports Authority, says, "We spend millions of hours manually verifying 'What is this? Who's it from? Where's it from?' Most people are leaning toward the RFID tag." He and others, however, are frustrated by what seems to be the intent of government agencies to experiment endlessly with new devices, new methods, and new rules for port security without reaching a decision. "They need to say, 'This is the standard. This is what you're gonna do.' And they need to do that within our lifetime."

A program that has lots of people wishing the government would just get on with it is TWIC, the Transportation Worker Identification Credential. That's an ID card the Transportation Security Administration intends to issue to all 12 million U.S. transportation workers—air and seaport employees, railroad workers, truck drivers, and so on—after each of them is subjected to a background and criminal-record check. The agency is testing smart and biometric cards in Philadelphia and Long Beach, Calif. Richard Steinke, executive director of the Long Beach Port Authority, says, "There are optical cards, thumbprint cards, retina cards—all kinds of ways for one's identity to show up." As part of one test, Steinke carries a card that brings up his photograph on an entry-point reader.

Common identification cards should help keep strangers away from containers and reinforce the difficult and important task of physically guarding the ports themselves. With operations spread over huge expanses of land and water, scattered cargo terminals, and often petroleum-tank farms, the ports are vulnerable. Disrupt the San Pedro harbor,

and you could block the ports of Los Angeles and Long Beach, which handle more than 40% of U.S. container imports.

Just one exploded vessel or a deftly aimed shoulder-fired missile could shut down most of the fourth-largest container port, Charleston. In the year ended last June, it handled about one million containers and had lots of other business: BMWs inbound from Germany (and outbound from the BMW plant in Spartanburg, S.C.); scrap and other raw materials headed toward Nucor's nearby mini-mill; and Norwegian Cruise Lines vessels sailing in and out of Charleston to the Caribbean. Concerns about Charleston go beyond commerce. About a fourth of the men and materials that headed for Iraq early this year left from one of its three Defense Department terminals.

So far, U.S. ports haven't gotten much in the way of federal help. The Transportation Security Administration has doled out \$282 million in grants covering 536 port security-improvement projects over the past two years. But that's not much more than the \$256 million it's given to just one airport, Los Angeles International, to improve security. Charleston has managed to snag Project Sea Hawk, a pilot program funded with \$5 million from the Department of Justice. Headed by Sean Kittrell, an assistant U.S. Attorney and anti-terrorism expert, Sea Hawk will explore ways that ports can get agencies to cooperate by sharing intelligence and manpower. Kittrell is bringing together representatives from about two dozen agencies and police forces who will work together in a harborside building. Some ship captains slowing to pick up a pilot on the way into Charleston Harbor have already found their vessel being boarded by a Sea Hawk team made up of sea marshals, Customs inspectors, and immigration officers.

Overall responsibility for ports and vessels everywhere in the U.S. still rests with the Coast Guard. Before Sept. 11, vessels gave the Coast Guard 24-hour notice of their arrival, along with basic information about ship, crew, and cargo. Since October 2001 the Coast Guard has required 96 hours' notice, with lots more information that it screens at its Intelligence Coordination Center in Suitland, Md. Last year the service's armed sea marshals boarded more than 12,000 arriving vessels, often intercepting them about 12 miles out to sea.

This year the Coast Guard issued new maritime security rules. One effect is that 10,000 U.S.-flag vessels, some 5,000 maritime facilities, 40 offshore platforms, and all 361 U.S. ports must have new security plans. The rules roughly match international requirements for ports and vessels adopted by 120 nations last year. But since some nations and some ships flying flags of convenience have a reputation for lax enforcement of rules, the Coast Guard intends to send its own people to review the plans of foreign ports and will check up on foreign vessels when they make their first stop in the U.S. Admiral Thomas Collins, commandant of the Coast Guard, estimates that the U.S. maritime industry will have to spend \$1.5 billion in the next year and some \$7 billion more over the next decade to comply with the new rules.

The Coast Guard is also starting to move on its Integrated Deepwater System, a \$10 billion, 20-year program under which it will be almost completely re-equipped. On the

way are new cutters, boats, planes, helicopters, unmanned aircraft, and advanced command-and-control systems to be delivered by a joint venture of Lockheed Martin and Northrop Grumman. Planned since 1998, Deepwater is supposed to be paid for with annual dollops of \$500 million in 1998 dollars. So far it's been shortchanged, but Congress upped the administration's proposal for fiscal 2004 to get it caught up.

Some experts worry about the danger of overreacting to a terrorist strike. Shutting down all the ports while Washington thinks things over would cause chaos and substantial damage to the American economy. However, the core problems are underfunding of the government's many programs and lack of speed in implementing them. The Coast Guard's Admiral Hereth claims that the "screens that the bad guy has to go through if he's coming from overseas are many and varied. He's going to have to do a lot of bobbing and weaving to get through the system." But there is lots left to be put in place before the screens are impenetrable. As George Weise, the former Customs commissioner, says, "I just hope it doesn't take a successful detonation of a shipping container to really make sure we take the necessary steps."