

# AVERTING DISASTER

## The Future of Cargo Security and How Supply Chain Managers Must Prepare

A publication of Manzella Trade Communications Inc.  
in association with the Mississippi World Trade Center



### *Executive Summary*

**A**fter the tragedy of September 11th, U.S. Customs and Border Protection (CBP) and its government partners implemented several intermodal cargo security initiatives to defend against an attack that could devastate the U.S. economy. Chief among these initiatives is a system designed to pinpoint and inspect cargo containers that may pose a terrorist threat.

The system in place today, however, must strengthen inherent weaknesses and evolve to meet economic, geographic, and political challenges of the next decade that threaten to constrain federal capabilities. Accompanying this evolution will be major changes in the two burdens that container targeting places on business: the 24-Hour Rule and cargo inspections. Supply chain managers must consider how the system will change if they hope to plan effectively for safe and efficient trade in the coming years.

In the weeks following 9/11, CBP had to employ an “implement and amend” approach to supply chain security, forming regulations quickly and adapting them over time. That adaptation has only just begun. Targeting and inspection processes must cope with the fact that maritime trade is expected to double by the year 2020, if not much sooner. Port space, throughput, and security funding already face limits in the United States and abroad. And political battles over security program results and annual budgets cast a cloud of uncertainty over the CBP layered approach to security.

Meanwhile, how CBP chooses to address several

system weaknesses could affect the entire targeting system and supply chain management. First, the 24-Hour Rule and maritime container targeting depend on the success of two related programs, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT), both of which face implementation problems of their own. CBP must overcome limitations in its information technology, particularly the Automated Manifest System and the new Automated Commercial Environment, for more effective targeting. And CBP must incorporate additional information in its computer targeting beyond vessel manifests, which do not present the most precise picture of a container and its contents in real time.

American companies must take greater responsibility for individual supply chain security using sound risk management principles. In light of federal changes on the way and the need to mitigate supply chain disruptions, supply chain managers should 1) join C-TPAT to reduce inspection risk; 2) divert shipments to safer channels to reduce inspection risk; 3) adjust inventory management to prepare for inevitable trade disruptions; 4) prepare for shipment data reporting earlier in the supply chain; and 5) prepare for broader document and data reporting requirements.

Because U.S. and global trade are truly one and the same, the protection of U.S. supply chains going forward will have to involve a more international effort that is best led by free-market industry, in conjunction with customs authorities.



**MANZELLA**  
TRADE COMMUNICATIONS, INC.

---

## Introduction: Diffusing the Bomb

**I**t's daybreak at a major Asian seaport and there's a dirty bomb in a shipping container. The sealed container looks exactly like the thousands of worn boxes that move in and out of the port each day on truck and train. And aside from a single lead-lined crate that conceals the deadly explosive, there is nothing sinister about this container's contents: name-brand consumer electronics and spare parts destined for Los Angeles. The container's ship, in fact, loads later this morning.

Security precautions among Pacific Rim trading partners have become tighter in recent months. Even a U.S. senator, during a photo-op at the same Asian port the week before, praised new efforts to safeguard supply chains. And yet, a huge cash bribe had been too much to resist for one truck driver on the mainland. Two days earlier he had turned a blind eye at a dark roadside stop as three men opened the container, loaded the crate from an adjacent truck, and resealed the container with a state-of-the-art mechanical seal. Within 10 minutes they had disappeared into the night and the container had resumed its journey to the busy port. Now a bomb sits in line for the gantry crane, undetected by overworked customs officers.

The bomb's detonator, assembled 10 months ago, waits patiently in an operative's apartment in Long Beach . . .

**T**his frightening scenario, completely fictional and yet all too plausible, is exactly the kind of nightmare that has weighed heavily on lawmakers, customs officials, and the global trading community since September 11th. It isn't difficult to see why intermodal trade is so appealing to the terrorist mind. For an enemy with the express goal of crippling Western economies, what better target than the very bloodstream of those economies? Ninety percent of the world's cargo moves by shipping

container. More than nine million containers arrive by sea in the United States each year, carrying more than 95 percent of the nation's non-North American trade by weight. The ubiquity of these identical containers that makes modern trade so efficient and cost-effective also makes it ripe for exploit. And a strike at the heart of the system would have disastrous consequences.

In a 2002 war game involving government and industry leaders, a dirty bomb scenario similar to the one above prompted decisions to close two U.S. ports for three days and all U.S. ports for nine days thereafter. During the first three weeks of the imaginary crisis, major stock indices plummeted, trading halted, gas prices spiked, and more than half of the *Fortune* 500 firms issued earnings warnings. As the game played out, it took three months to clear the container backlog resulting from the closings, with a total cost to the U.S. economy of \$58 billion.<sup>1</sup> Another study estimates that costs following a detonated weapon of mass destruction shipped by container could reach \$1 trillion.<sup>2</sup> "A successful attack would make us all victims," says Christopher Koch, president and CEO of the World Shipping Council. "It would affect every supply chain, every carrier, every port, and every nation's trade and economy."<sup>3</sup>

In the days following 9/11, the U.S. Customs Service—reorganized in 2003 as U.S. Customs and Border Protection (CBP)—began to implement a host of trade security initiatives with its government partners and its new parent organization, the Department of Homeland Security (DHS). Those initiatives continue to expand in scope and authority more than three years after 9/11, in harmony with similar safeguards around the world. In general,

---

### A Note from the Publisher

Although the publisher, Manzella Trade Communications Inc., has made all reasonable efforts to ensure the accuracy of this report and its contents, the publisher cannot guarantee the accuracy of every source cited herein. All opinions given, unless cited otherwise, are expressly those of Manzella Trade Communications and not those of any sponsor or distributor of this report. No part of this report should be construed as specific advice for any firm, which must consider a range of unique business variables beyond the scope of this report.

Manzella Trade Communications Inc. is a strategic communications consultancy that provides integrated custom publishing, public affairs, public relations, and consulting services. President and publisher: John Manzella. Report author: James Burroughs. For more information, visit [www.ManzellaTrade.com](http://www.ManzellaTrade.com).

All rights reserved by Manzella Trade Communications, Inc. (© 2005). PO Box 1188, Williamsville, NY 14231-1188 U.S.A.  
Phone 716.681.8880 ext. 239 • Fax 716.681.6888 • [Info@ManzellaTrade.com](mailto:Info@ManzellaTrade.com) • [www.ManzellaTrade.com](http://www.ManzellaTrade.com)

---

security measures are designed to impede the two most-feared terrorist approaches to supply chains: 1) the “hijack” scenario, like the one above, in which terrorists intercept a legitimate shipment and tamper with it; and 2) the “Trojan horse” scenario, in which a terrorist organization usurps or develops a legitimate trading identity to ship dangerous cargo.<sup>4</sup> Yet, because there is no single system that governs the global movement of containers—it is instead an amalgam of thousands of business and government entities—developing a seamless defense is impossible without bringing trade to a grinding halt. The approach must instead be one of prioritizing risks and managing them with finite resources.

The Department of Homeland Security’s “layered” approach to supply chain security is a combination of programs and initiatives spearheaded by CBP and related agencies. Implemented at different times, with different methodologies, and with different goals, the measures often overlap one another in their attempt to protect a vast, multifaceted industry. One of the earliest such efforts following 9/11 was the formation of a system that could target U.S.-bound maritime shipping containers posing a terrorist threat. In effect, by pushing the U.S. border across the oceans, CBP could inspect high-risk containers before they departed for America, where traditional dockside inspection of a dangerous shipment might be too little, too late.

Gradual implementation of these targeting and prescreening efforts, as follows, laid the groundwork for the familiar system in place today.

- *November 2001:* CBP establishes the National Targeting Center (NTC) in Washington, D.C., to conduct cargo targeting in coordination with the intelligence community.
- *January 2002:* CBP announces the Container Security Initiative (CSI), a program designed to identify and examine high-risk containers at foreign ports with the cooperation of foreign customs agencies.
- *June 2002:* The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 becomes law to protect food and drug imports. Administered by the Food and Drug Administration (FDA) and jointly enforced by CBP, the Act requires that advance notice be given to the FDA prior to all food imports.<sup>5</sup>
- *August 2002:* As part of its Sea Cargo Targeting Initiative, CBP modifies its Automated Targeting System (ATS) computer model. Originally designed to identify illegal narcotics in container shipments, ATS incorporates terrorism-related targeting tools to look for red flags in shipping manifests, combined with intelli-

gence, suspicious trading patterns, and warnings from other government agencies. CBP also standardizes procedures for handling high-risk shipments.

- *December 2002:* To make shipment data available to CSI inspectors overseas in time to prescreen cargo before departure, CBP implements the “24-Hour Rule.”<sup>6</sup> Sea carriers and/or automated non-vessel-operating common carriers (NVOCCs) begin submitting vessel manifests to CBP 24 hours before lading at foreign ports. Enforcement begins in February 2003. Generic cargo descriptions on manifests are prohibited, and carriers whose descriptions are found to be inaccurate are held liable.
- *May 2003:* CBP begins sending “Do Not Load” orders in response to invalid cargo descriptions. CBP ports are authorized to issue monetary penalties for 24-Hour Rule violations.
- *January 2004:* The Required Advance Electronic Presentation of Cargo Information rule, pursuant to the Trade Act of 2002, extends the advance manifest filing requirement to incoming and outgoing trade by air, truck, and rail carriers, though the advance notice for these other modes of delivery is only a matter of hours prior to arrival in the United States.
- *March 2004:* Sea carriers and/or automated NVOCCs are required to submit an electronic cargo declaration using the Sea Automated Manifest System. Full enforcement begins in July 2004, including denial of preliminary entry, issuance of penalties at each port of arrival, and denial of unloading.

CBP and its partners have little choice but to use such high-tech methods to find the poisoned needle in the haystack, since the enormous volume of maritime imports coupled with the agency’s limited resources make it impossible to inspect each arriving container manually. Although, at present, CBP inspects only 5 percent of imported maritime containers, the agency insists that it prescreens 100 percent of the manifests of incoming vessels and thus, somewhat indirectly, the contents of each container before lading overseas. Meanwhile, in the United States, the agency is providing all ports of entry with radiation-detection portals, through which each inbound container moves before leaving the port for U.S. destinations. Inspectors may also carry detection devices as a second way to discover smuggled radioactive material, though neither method is foolproof.<sup>7</sup> U.S. and foreign customs officers may employ similar technologies overseas, though the rate of implementation is slower than it is in the United States.

If at any point officials decide a container warrants

further attention, they might first use non-intrusive inspection equipment such as the Vehicle and Cargo Inspection System (VACIS) to look for any visual anomalies without opening the container. (Such systems, which employ x-ray or gamma ray radiation, are not perfect, either.) Whether or not inspectors first use a VACIS-like system, they can choose to open a container and examine it manually if prescreening has aroused suspicion. Such an inspection could delay a shipment by one day or more.

But does this system of targeting and prescreening as it stands today actually work? The fact that three years have elapsed since 9/11 without a trade-related terrorist incident is not enough, by itself, to prove the system is effective, especially given the patience and advance planning of enemies

like al-Qaeda. CBP has done an admirable job of converting customs methods to today's threat of global terrorism in a relatively short time; yet to achieve measurable improvements in targeting, further changes in the overall CBP strategy

must occur. For example, a 2004 report by the Government Accountability Office (GAO)<sup>8</sup> states that the current CBP strategy does not fully incorporate all necessary elements of a risk management framework needed if the agency is to achieve optimum results with limited resources. In addition, the report says, the CBP strategy and ATS are not fully consistent with recognized modeling practices, such as the incorporation of additional trade documentation and the widespread use of random inspections.<sup>9</sup>

The bottom line for supply chain managers, therefore, is that CBP and international efforts are only beginning, and the evolution of cargo targeting will have serious and costly implications for all businesses engaged in world trade in the future. Already the 24-Hour Rule ("the Rule") and container targeting in general have added significant new costs throughout supply chains, such as investments in information infrastructure, new personnel hiring and training, delays due to inspection, container backlogs at departure ports, documentation fees, liabilities and fines, increased lead times, and increased inventories. These costs are likely to continue and expand as the Rule changes over time. According to one study, the estimated annual cost of the Rule could range from \$280 million up to \$10

billion.<sup>10</sup> Tempering this amount are the cost benefits that some firms will realize from reduced cargo theft and pilferage, which total in the billions of dollars annually, as well as significant increases in supply chain visibility and logistics efficiency.

Meanwhile, government costs also are expanding, as is the debate concerning the appropriate level of federal spending for supply chain security. The 9/11 Commission has pointed out, for example, how more than 90 percent of the government's annual \$5 billion investment in the Transportation Security Administration goes toward passenger aviation—"to fight the last war," despite the reality that "opportunities to do harm are as great, or greater, in maritime or surface transportation."<sup>11</sup> Others

have criticized a lack of long-term funding strategies for such essential programs as CSI, while ports continue to shoulder the burden of what they call an unfunded port security mandate. Such debate over federal funding may continue, ironically,

---

*The bottom line for supply chain managers, therefore, is that CBP and international efforts are only beginning, and the evolution of cargo targeting will have serious and costly implications for all businesses engaged in world trade in the future. Already the 24-Hour Rule and container targeting in general have added significant new costs throughout supply chains.*

---

as long as world commerce eludes a direct terrorist attack, since loose purse strings in Congress have proven to be largely behind the curve when it comes to homeland security.<sup>12</sup>

The purpose of this report, however, is not to critique the approach of the Department of Homeland Security and its agencies toward supply chain security, to evaluate its spending priorities, or to determine the effectiveness of security initiatives. Nor is its purpose to explain the day-to-day workings of the now familiar 24-Hour Rule, in operation since December 2002. It is instead designed to provoke discussion about how and why maritime cargo targeting, in particular, will evolve over time due to 1) economic, geographic, and political forces of the next decade and beyond, and 2) CBP measures to strengthen inherent weaknesses in the system as it stands today. Accompanying this evolution will be profound changes in the two burdens that targeting places on business: the 24-Hour Rule on the front end of shipments, and cargo inspections on the back end. Only by considering these changes will supply chain managers be able to plan effectively for safe and efficient trade in the coming years.

---

## Targeting and the Trade Environment of the 21st Century

Since day one, as world traders and CBP alike will admit, the 24-Hour Rule and container targeting have been far from perfect in design and implementation. In the weeks following 9/11, CBP didn't have the luxury of time in formulating a grand design for cargo security. Instead, the agency had to use an "implement and amend" approach, getting regulations on paper quickly and adapting them as real-world conditions dictated. That adaptation has only just begun. Current economic, geographic, and political trends indicate that the world trade environment only a short time into the future will be very different than it is today. And that's in a good scenario—one without a major terrorist strike at intermodal commerce. If the United States and its trading partners are to protect supply chains and keep trade flowing smoothly, today's container targeting and inspection capabilities must deal with enormous challenges ahead.

### 1. Increasing Trade Volume

To begin, the tide of imports into the United States is rising quickly. U.S. industries expect maritime trade to double by the year 2020, while some economists have predicted that doubling may occur as early as 2014 due to marketplace demands.<sup>13</sup> Already ocean container inspection rates have increased from less than 2 percent before 9/11 to between 5 and 6 percent, meaning that CBP inspects at a current rate of 400,000 or more containers each year.<sup>14</sup> Meanwhile, there is great political pressure to increase the number of inspections further, especially among lawmakers trying to appear tough on homeland security during election years.

Even at current rates of inspection and trade growth, will CBP have the personnel and resources to inspect one million containers annually by 2014 and still keep trade flowing smoothly? Will the 24-Hour Rule and ATS as they stand today be able to provide and process enough information to pinpoint threats before ships depart foreign ports? Looming over these questions is the fact that a successful attack on maritime commerce, a thwarted attempt, or even a severe threat based on credible intelligence would likely trigger a sudden, sharp increase in the rate of inspections that might never subside. Backlogs of suspect containers waiting for inspection both overseas and in U.S. ports could be a very real possibility.

High-tech, non-intrusive inspection technologies are an oft-mentioned solution to inspection delays, but the systems alone aren't a complete answer. Crowded port terminals, mechanical breakdowns, bad weather, and safety concerns of longshoremen at some ports are among

the constraints on these technologies.<sup>15</sup> And they simply can't detect all kinds of weapons, all the time. The simple, hard truth is that CBP will require corresponding increases in its budget and workforce to keep pace with the need for more inspections.

Targeting and inspection initiatives will have to reach out to international partner agencies in a standardized effort to protect more trade. Programs designed to increase supply chain security and decrease targeting risk, such as the Customs-Trade Partnership Against Terrorism, will require additional resources to respond to the higher trade volumes. And the CBP information network and the data it requires from private industry (i.e., the 24-Hour Rule) will have to expand for the timely, precise prescreening of millions of additional containers.

### 2. Limited Port Capacity

Aside from the implications for importers who depend on the timely delivery of their inventory, inspection backlogs are an alarming prospect simply because there isn't room for them. Diminishing space and finite port throughput in urban areas in the United States and abroad are a growing problem. Increased inspections will further reduce the productivity of space-starved ports, translating into larger backlogs and wait times. The Port of Long Beach, for example, recently phased in longer operating hours, including nights and weekends, as a way to increase terminal capacity and reduce daytime trucking congestion. The port will offset the cost of weekend and night operations by assessing a \$20 fee on all loaded international containers.<sup>16</sup> As trade volumes continue to rise, smaller ports will have to take on an increasing amount of trade diverted from megaports operating at capacity. Ports of all sizes around the globe are in need of massive investment in infrastructure, dredging to accommodate larger vessels, and more personnel to cover expanded operations based on trade growth alone. New security mandates and increased inspections only exacerbate the need for expansion and investment.

Yet sustained government assistance for ports is far



from certain, as demonstrated by widely divergent views in Congress and the executive branch over who should pay and how much. Between 9/11 and September 2004, the DHS Port Security Grant Program provided ports with a total of some \$488 million in grants divided among four rounds—despite the fact that the U.S. Coast Guard has estimated that port investments needed for compliance with the Maritime Transportation Security Act will be \$1.125 billion in 2004–05 and an additional \$5.4 billion over the next 10 years.<sup>17</sup> The four rounds of grants have diminished markedly from \$179 million in the first round, to \$168 million, \$92 million, and \$49 million in subsequent rounds. “Without adequate help, ports will struggle to make the needed [security] improvements,” says Kurt Nagle, president of the American Association of Port Authorities. “Ports are already diverting funds from other infrastructure improvements necessary to meet the continuing growth in trade, which is expected to double or even triple in certain ports over the next 10 years.”<sup>18</sup>

---

*Smaller ports in the United States and overseas will have to process a growing share of trade in the years ahead, yet these ports today are unable to accommodate such volume in a secure manner. U.S. ports of all sizes will have no choice but to pass along much of the cost of expansion and security in the form of higher user fees, a trend already underway.*

---

Again, the hard truth comes down to time and money. Smaller ports in the United States and overseas will have to process a growing share of trade in the years ahead, yet these ports today are unable to accommodate such volume in a secure manner. U.S. ports of all sizes will have no choice but to pass along much of the cost of expansion and security in the form of higher user fees, a trend already underway. Furthermore, limits on how much trade U.S. ports can process will place new pressure on CBP to prescreen and inspect more containers on foreign soil, meaning costly expansion for programs like CSI. Ports around the world face similar challenges of space and throughput, however. To cope with potential container pileups at foreign ports, the filing of shipment data and cargo targeting will need to move back in the supply chain—from today’s 24 hours before lading toward the time of container stuffing and sealing.

### 3. Uncertain Political Support

As shown by the port security example, Washington expects industry and, ultimately, American consumers to pay their share of supply chain security. It’s fair to ask the private sector to bear part of the cost, since it profits from secure and efficient trade. On the other hand, because of

the threat that a trade-related terrorist incident poses to the general public and the U.S. economy, the government also has a responsibility for general protection. The problem, however, is that no one knows what their share of the cost is, because federal authorities have been too vague, or downright evasive, when it comes to clearly defining public versus private responsibilities in supply chain security.<sup>19</sup>

In addition, political support for even basic security initiatives related to supply chain security is far from guaranteed throughout changing U.S. administrations and congressional election cycles. The same can be said for the cooperation of foreign governments and customs agencies, on whom the success of any comprehensive cargo security effort depends. Some observers on Capitol Hill, for example, have already expressed skepticism over federal

efforts to strengthen trade security since 9/11.<sup>20</sup> One such program, Operation Safe Commerce (OSC), was championed by some members of Congress and derided as pork-barrel spending by others. Although the research initiative achieved its mission and compiled

a final report, for two years the Bush administration and congressional advocates often sparred over funding and the program’s very existence. With America’s post-9/11 bipartisan unity now a thing of the distant past, political squabbling over program results and annual budgets threatens to undermine the layered approach to security. If one of the layers like OSC should falter under political pressure, what would be the effect on related initiatives, such as CSI and the 24-Hour Rule?

Keeping cargo security focused and well funded will require consistency among future DHS administrations and effective performance measures for winning over Congress. But the alarming misunderstanding of logistics issues in Washington begs the question of whether or not Congress will ever truly “get” cargo security.<sup>21</sup> More government openness to industry leadership, allowing companies who trade to take on more responsibility for protecting the system, could be one solution that achieves better, more cost-effective results. As security efforts threaten to grow beyond federal coffers in budget-conscious times, it may also be time to call on U.S. allies in trade to take on more of the task and foot more of the bill. A global standard uniting world customs agencies into one system may be an idea whose time will come.

---

## Four Objectives for a Stronger Targeting System

**A**mid this geopolitical backdrop of the coming decade, CBP also has issues to contend with that hit closer to home. In the urgency of adoption, the 24-Hour Rule and container targeting inherited a number of weak points that the agency must shore up if it is to achieve its goal of efficient supply chain security. Many early speed bumps in the Rule itself, common with almost any new regulation, continue to work themselves out during daily practice. These have included issues of confidentiality, the participation of NVOCCs in advance filing, acceptable cargo descriptions, and the phase-in of automation. Underneath these relatively minor problems, however, are more fundamental questions that require deeper, long-term planning. How CBP chooses to address them could have significant effects on how the entire targeting system functions, and how it affects supply chain management.

### 1. Keeping CSI Strong Indefinitely

The effectiveness of the 24-Hour Rule and maritime container targeting depends on the success of two related programs, the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). Yet these initiatives face implementation problems of their own.

At the heart of CBP's pushing-out-the-border strategy, CSI is founded on four core elements: 1) using intelligence and automated information to identify containers that pose a risk for terrorism; 2) prescreening those containers at the port of lading before they arrive in the United States; 3) using non-intrusive detection technology whenever possible to examine suspicious containers; and 4) using smarter, tamper-evident containers. CSI places CBP officers at major world seaports to work with foreign colleagues in identifying and examining high-risk containers, using data gathered under the 24-Hour Rule and run through ATS. Without the Rule, CSI can't work. Conversely, without an effective CSI overseas, the data supplied by carriers under the Rule does nothing to mitigate terrorist threats before it's too late.

As of October 2004, 16 countries had entered into bilateral CSI agreements with the United States, with the program operational at 31 of the world's major seaports in Europe, Asia, Africa, and North America. Ultimately, CBP envisions having CSI teams at 40 or more ports, covering more than 80 percent of all containers shipped to the United States. But CSI must be adequately staffed and funded if it is to process the increased trade flow expected

over the next decade. The GAO believes CBP will have a difficult time staffing long-term overseas posts with qualified, highly skilled personnel, much the same way the State Department has trouble staffing positions in hardship posts.<sup>22</sup> Currently CBP sends teams of four to eight inspectors on temporary duty assignments of only three or four months because DHS has not authorized longer assignments.<sup>23</sup>

While on paper CSI appears to accomplish much in deterring terrorist attacks, CBP still lacks hard-data measures of the program's effectiveness.<sup>24</sup> This despite the fact that the annual budget for CSI has ballooned. Spending will have to keep pace with the necessity of enrolling additional world ports, but will an easily distracted Congress stay on board? Lawmakers will want to see more inspections with more tangible results—that is, evidence of thwarted attempts at terrorism. Only by keeping talented officers in position and presenting a positive return on investment can CBP guarantee congressional support for this program so crucial to intermodal cargo security.

### 2. Taking C-TPAT to the Next Level

C-TPAT is a voluntary, joint government-business initiative that asks participating importers, carriers, brokers, warehouse operators, and foreign manufacturers to ensure the integrity of their security practices and those of their partners within the entire supply chain. In exchange for C-TPAT membership, companies receive the benefit of lower container targeting risk in ATS and fewer inspections. From the perspective of private business, C-TPAT is the primary means for avoiding delays and keeping goods moving efficiently. From CBP's perspective, it is a principal way to reduce the risk of most U.S. imports (at least on paper), thereby helping the agency manage the number of inspections required as the volume of trade increases.

As of September 2004, C-TPAT membership had surpassed 7,000 companies, including most major U.S.



importers, accounting for more than 50 percent of maritime cargo by value.<sup>25</sup> On the plus side, these largest importers who own or operate the entire supply chain route from start to finish experience the fewest security problems because of the greater control they exert. Most smaller importers don't have that option, however, and rely on several small logistics providers. Studies show that cargo security is affected negatively by the number of smaller individual companies used to move cargo. If it hopes to provide a comprehensive umbrella of U.S. supply chain security, C-TPAT will have to reach out to more of these smaller firms, foreign manufacturers, and foreign logistics providers. That means thousands of additional members from all around the world.

As voluntary membership rapidly approaches the 10,000 mark, however, the effectiveness of C-TPAT as it stands today could be facing its breaking point. Initial and continuing audits of members' security practices will remain a stiff

challenge to limited CBP resources. And no one can predict how often a dangerous security lapse might occur at an unvalidated member operation (or even a validated one), or how easily a terrorist group might infiltrate and exploit such an

operation with an overstretched CBP not paying attention. As with CSI, there is no quantifiable evidence yet that C-TPAT even does what it sets out to do.

Already some in the maritime industry have shown a wavering commitment to the program. "Some participants continue to strongly adhere to the program's goals out of a sense of responsibility, while others, driven by their bottom line, are moving away from the program and are only meeting those requirements in law or regulation," says Sen. John McCain, R-Ariz.<sup>26</sup> Simply put, because the program attempts to encompass container stuffing, sealing, and land-based transport overseas—perhaps the most vulnerable phases in a container's journey—it may be too important to be based on a "trust-but-can't-confirm" approach to best practices among members. Without tighter government oversight of a program that results in lower targeting risk, the opportunity for terrorists to exploit a member company's preferred status seems too great. Simultaneously tightening and expanding C-TPAT,

however, will only make the program significantly more expensive, on top of already increasing annual budgets in times of deficit.

If a truly effective C-TPAT threatens to grow beyond CBP capabilities, one possibility is to allow the program to evolve out of government hands into an innovative alternative run by private industry. As one expert points out, the Maritime Transportation Security Act required the evaluation and certification of secure systems of intermodal transportation. The law did not specify that these programs be conceived or implemented by the federal government.<sup>27</sup> It could be that a global trade association funded by its membership, for example, could better reach supply chain players around the world, in coordination with CBP and foreign customs agencies. A less extreme alternative would be for C-TPAT to spawn identical programs for other world markets that together would form a single international standard, under the

oversight of the World Customs Organization. CBP Commissioner Robert Bonner already has suggested such a framework for the future, including global versions of the 24-Hour Rule, CSI, and ATS.<sup>28</sup> Under this framework, all participating nations would require the same advance shipment

data; nations would apply the same risk management approach to targeting high-risk containers; customs agencies would share information about terrorist risks to intermodal trade; and participating countries would agree to expedite processing for companies who meet C-TPAT-like best practices for supply chain security. Of course, conservatives in Congress will not like an idea that, on the surface, appears to cede authority for homeland security to a global body. For such a system to gain acceptance, it will have to play up the advantages of a global infrastructure in data gathering and targeting (i.e., scope and resources beyond the capability of any one nation) but recognize the autonomy and flexibility of national customs enforcement.

Now that the urgent days of initial implementation are over, CBP will have to concentrate on more long-term planning, transparent to U.S. firms and lawmakers, for both CSI and C-TPAT. As of the most recent GAO assessment of both programs, for example, CBP had not developed a human capital plan that addresses long-term

---

*If the war on terror is to be a protracted global fight, as Washington has insisted, then these initiatives designed to protect America's soft underbelly must achieve the same level of untouchable importance across administrations that various government institutions—military, intelligence, codework—received during the Cold War.*

---

staffing needs such as recruiting, training, and retaining the highly specialized personnel needed by both programs.<sup>29</sup> Such long-range plans are already underway, CBP says, as are program effectiveness reviews by the DHS Office of Inspector General. Congress has insisted on a report on these and other programs by February 2005.

If the war on terror is to be a protracted global fight, as Washington has insisted, then these initiatives designed to protect America's soft underbelly must achieve the same level of untouchable importance across administrations that various government institutions—military, intelligence, codework—received during the Cold War. Congress, the fledgling Department of Homeland Security, and our international customs allies have a long road ahead in making that happen.

### 3. Broadening the Power of Automated Systems

The 24-Hour Rule and container targeting also depend on various imperfect systems to get data from carriers overseas to the ATS computer. First among them is the Automated Manifest System (AMS), a multi-modular cargo inventory control and release notification system through which carriers submit their electronic cargo declaration 24 hours before lading. AMS began in the mid-1980s as an experiment intended to accelerate the flow of commerce. It is now being turned into a security tool, a task for which it was not designed and for which it is only partially suited, according to one expert.<sup>30</sup> As the system evolves to incorporate new security goals, it continues to present inconveniences to the trade and more serious roadblocks to information gathering. For example, AMS cannot accommodate consolidated shipments without the entry of separate bills of lading, nor can it allow prescreening to be done at the first port of lading for transshipped cargo. Also, because of the design of AMS, importers, shippers, and forwarders—who possess the most accurate knowledge about foreign manufacturers, the information most useful in container targeting—cannot participate in advance filing.

AMS was originally part of the Automated Commercial System import network, designed in 1984 but more recently unable to meet the increasingly complex, long-term requirements posed by growth in trade, enforcement responsibilities, and security threats. Many of the limitations in AMS may be corrected, CBP says, with the evolution of the Automated Commercial Environment (ACE), a massive Customs modernization project that prompted congressional bickering for years before finally getting underway. As a replacement system, ACE will “revolutionize” how CBP processes commercial import and export data, the agency says, and will be a critical element in preventing



cargo from becoming an instrument of terrorism.<sup>31</sup> Having evolved already to incorporate security features since its original design, ACE and its Secure Data Portal will be implemented in phases to all CBP ports of entry over the next four years—a process known thus far for running over budget and behind schedule.<sup>32</sup> CBP has stated that as the various releases of ACE are completed and the ability to collect data and information is enhanced, it will reevaluate related aspects of the 24-Hour Rule. As with any evolving software system, such updates and reevaluation—and subsequent effects on the Rule—can be expected to continue far into the future, subject to changing trade conditions, world events, the globalization of customs security standards, and budgetary politics.

### 4. Giving ATS More Valuable Data

The effectiveness of high-risk container targeting can only be as great as the data the 24-Hour Rule provides to ATS. Currently, ATS relies chiefly on vessel manifests, extracted from individual bills of lading and supplied by carriers once a container comes into their possession, or soon before. ATS matches its targeting rules against 14 manifest data points and other available data, such as intelligence reports, for each incoming container, then assigns a level of risk to each shipment. Although the 24-Hour Rule did successfully eliminate generic cargo descriptions such as “FAK” (freight all kind), “general cargo,” and “STC” (said to contain) that made precise targeting impossible, the manifest data as currently provided still has serious limitations when it comes to ferreting out suspicious containers.

First, although improved in quality and timeliness,

manifest information still is not always accurate.<sup>33</sup> Second, terrorism experts, members of the international trade community, and even CBP inspectors have characterized a ship's manifest as one of the least reliable or useful types of information for targeting purposes, according to the GAO. Accordingly, if ATS input data are poor, the system's outputs, or risk-assessed targets, are not likely to be very good.<sup>34</sup>

At the heart of the problem is the fact that the carrier has little knowledge of the loading and transportation history of a sealed container (which it is unable to inspect) beyond the assurances of the customer. In fact, the container may have been vulnerable to tampering several times in the days or even weeks before delivery to the carrier, with such vulnerability virtually unknown to CBP for the purposes of targeting. That's because bills of lading may not indicate where goods actually originated, nor will they always contain information about intermediate handling or where a shipment may have stopped prior to arriving at the port of lading. CBP attempts to address these vulnerabilities in the earlier stages of a container's journey by relying on the past record of trusted shippers and through C-TPAT best practices. For example, even though a carrier may not exercise control over the sealing of containers, carriers that join C-TPAT are "expected to promote effective security measures throughout the entire supply chain."<sup>35</sup> Besides placing an inordinate amount of liability on carriers, this approach only gives assurances about the companies in possession of a container. It does not offer specific information about the packing and shipping history of individual containers. Even legitimate cargo from legitimate shippers could fall prey to terrorists patient enough to learn supply chain weaknesses.

"I have little doubt that al-Qaeda possesses the means to identify those users of the maritime transportation system that U.S. authorities currently view as low security risks," says Stephen E. Flynn of the Council on Foreign Relations. "I also believe that they are fully capable of exploiting the many opportunities to intercept and compromise these legitimate shipments either at their point of origin or anywhere along the transportation route they travel."<sup>36</sup>

CBP continues to look for ways to improve the quality of the limited information that currently feeds ATS, but clearly ATS must incorporate additional types of information in order to identify a wider range of suspicious containers. Future targeting will expand by incorporating

data—both documents and right-time readouts from "smart" containers—that will give CBP a complete picture of the risk a particular container might

pose. As discussed below, this will require supply chain managers to invest in information infrastructure and new technologies that make business documents and container status information available to CBP for targeting on demand.

CBP may also choose to expand the 24-Hour Rule to include empty containers and bulk cargo, currently exempt, as well as all break-bulk cargo without exceptions.<sup>37</sup> Certain bulk cargo, such as petroleum products and ammonium nitrate, are inherently dangerous, and empty containers and break-bulk cargo, while more transparent to CBP officers than a sealed container, still present opportunity for concealment. As supply chain security tightens in intermodal trade, terrorists may examine these cargos as possible areas of weakness

available for exploit, unless CBP imposes new security measures first.

Across the board, CBP also will have to conduct more simulated tests of ATS to pinpoint weaknesses and determine how

best to make improvements. As of March 2004, the only such tests known to the public were two conducted by ABC News without CBP's knowledge. In both cases, the network sealed depleted uranium inside a lead pipe loaded into a U.S.-bound container. Although CBP targeted the containers as high risk, the non-intrusive VACIS inspections did not detect a visual anomaly in either container, so CBP did not open them for further inspection.<sup>38</sup> Additional CBP efforts to test the effectiveness of ATS will involve more random inspections. Already CBP has a program in place called the Supply Chain Stratified Examination, which randomly selects containers for examination from among those deemed low risk by ATS. Learning from inspection results will allow the system to evolve and improve, and the random approach may also provide an added layer of deterrence.



---

*Future targeting will expand by incorporating data—both documents and right-time readouts from "smart" containers—that will give CBP a complete picture of the risk a particular container might pose.*

---

---

## Preparing for Change: Five Action Points for Supply Chain Managers

So what will these global trends and likely CBP actions mean to supply chain managers in the years ahead? And how should they prepare?

First, assuming a constant terrorist threat to commerce, the number of container inspections will increase significantly around the world. CBP's goals of expanding CSI and making container targeting more effective also will place a greater informational burden on businesses. The agency's dual objective of efficient trade, however, will depend in part on the capacity of world ports, an effective C-TPAT program, and long-term congressional spending for its initiatives—none of which are guaranteed at a level that will match U.S. import growth. As federal cargo security efforts evolve, shippers, importers, and logistics providers must take proactive steps to mitigate shipment delays and prepare for the filing of more detailed shipment data. Furthermore, companies of all sizes must take adequate steps now to avoid a logistics crisis in the event of a successful attack on America's trade infrastructure. All spending and advance planning must be conducted under a prudent risk management framework, but action of some kind is vital. Those who choose to do nothing at all could be risking the very future of their business.

In addition to other, more general supply chain security practices and costs, U.S. companies should consider *at least* the following five action points relating to the 24-Hour Rule and the targeting of maritime containers:

- Join C-TPAT to reduce inspection risk;
- Divert trade to safer channels to reduce inspection risk;
- Adjust inventory management to prepare for inevitable disruptions;
- Prepare for shipment data reporting earlier in the supply chain; and
- Prepare for broader document and data reporting requirements.

### Action Point #1: Join C-TPAT to Reduce Inspection Risk

As CBP has refined ATS, the inspection rate for all containers entering the United States has increased from 7.6 percent before 9/11 to 12.1 percent just two years later, "and it is rising," according to CBP Commissioner Robert Bonner. Sea container inspections have nearly tripled over the same period.<sup>39</sup> Each new inspection adds time and cost to supply chains with little room for either.

Consider just one example at the Packer Avenue Marine Terminal in Philadelphia. There CBP inspects approximately 50 to 80 containers a week using non-intrusive



VACIS technology. Depending on the arrival of the vessels and the availability of the VACIS equipment, these "quick" inspections could take several days. Holding a container for a full manual inspection can delay the release of the cargo an additional five days.<sup>40</sup> Delays and costs at overseas ports can be even greater.

Projected trade growth and the practical need for more random inspections, as described above, will be the two primary drivers behind increasing inspections in the years to come. Also fueling the increase will be the fact that container inspections have become the easy political answer to questions of port security. Whereas CBP inspections rarely used to make news, with the exception of a record-breaking drug bust here or there, today lawmakers hold press conferences at major ports and talk tough on trade security. (During the 2004 presidential race, both President George W. Bush and Sen. John Kerry held such events. At one in Palm Beach, Fla., Kerry said that inspections should increase to a "significantly higher level."<sup>41</sup>) Whether or not politicians have completely considered the logistics and funding demands of inspection increases is beside the point. As long as the idea lends itself so easily to sound bites, lawmaker interest will continue to foster an environment conducive to more inspections.

Businesses who want to reduce their exposure to targeting risk and more inspections can do so only by becoming a familiar, trusted, and prudent trader in the eyes of CBP and its ATS computer. That means establishing a good security track record and making sure that all supply chain partners have done the same. Currently the only way to achieve most of this at one time is through membership in C-TPAT. Although C-TPAT faces a number of long-term challenges, as discussed above, adherence to the voluntary program's standards remains the primary way

that businesses can reduce their targeting risk, outside of the unforeseen random inspection. In addition to receiving lower risk scores, members who subscribe to program standards may also receive breaks on penalties and damages for violations of the 24-Hour Rule.<sup>42</sup> As long as these benefits continue, membership in C-TPAT only makes good sense, despite the costs. Furthermore, those companies who assume an active role in the program now may have increased leverage in steering the evolution of C-TPAT, including laying the groundwork for an international initiative based on the C-TPAT model.

But C-TPAT benefits are only the icing on the cake for companies who have invested in the security of their supply chains. Strong adherence to, and furtherance of, industry best practices of security also ensure against the ultimate risk: that a single security lapse in one company's supply chain, if that lapse leads to disaster, could condemn all future shipments. An entire firm could become a pariah to both its trading partners and world customs authorities—a certain recipe for doom.

---

*Strong adherence to, and furtherance of, industry best practices of security also ensure against the ultimate risk: that a single security lapse in one company's supply chain, if that lapse leads to disaster, could condemn all future shipments. An entire firm could become a pariah to both its trading partners and world customs authorities—a certain recipe for doom.*

---

## Action Point #2: Divert Trade to Safer Channels

From its beginning in the months following 9/11, CSI focused on implementation at the 20 largest overseas ports, which ship around two-thirds of the United States' annual incoming container volume. With that goal achieved, CBP has begun placing inspectors at smaller, high-risk ports throughout the world.

Despite original reservations about CSI from the European Union (EU), which feared that CSI ports in Europe would have an economic advantage over non-CSI ports, the EU and DHS signed an agreement in April 2004 outlining future cooperation in expanding CSI. DHS has received similar pledges from the G8 countries and the World Customs Organization (WCO), allowing ports in all 161 WCO member nations to develop programs along the CSI model—if they can afford the required infrastructure and non-intrusive inspection technology. As of October 2004, the number of CSI ports worldwide was 31 and counting.

CBP hopes to expand the program to cover more than 80 percent of all containers shipped to the United States. The question then arises: How will the other 20 percent be

treated? Without a CBP presence or standard security measures in place at non-CSI ports, containers laded at those ports should receive higher risk scores in ATS. In other words, as CSI expands as both a U.S. and global initiative, containers originating outside the circle of "friendly ports" will be subject to higher targeting risk, increased inspections, and more shipping delays. Furthermore, in the event of a maritime terrorist attack anywhere in the world, seaports not participating in CSI will experience much longer delays in resuming cargo operations.<sup>43</sup>

Thus, U.S. importers currently working through non-CSI ports in any region of the world should consider diverting shipments to the nearest CSI port. While changing suppliers or altering land transportation overseas could add additional time and cost to a supply chain, these

consequences must be weighed against the cost of routine delays, frequent inspections, and even an indefinite halt in trade that might occur with commerce through a non-CSI port. That being said, it should be noted that shipping goods from a CSI port does not alone offer any

guarantee against delays. The very idea of inspecting containers overseas instead of in the United States, in fact, adds great uncertainty to product delivery, as a study cited below indicates. CSI merely offers the lesser of two risks.

On a related note, as of July 1, 2004, ports and vessels worldwide were required to be compliant with security plan regulations imposed by the International Ship and Port Facility Security Code. While compliance among the world's more than 9,000 ports was only 69 percent as of July 1, that number had improved to 89.5 percent by early August, according to the International Maritime Organization. Compliance for affected vessels was well over 90 percent by August.<sup>44</sup>

In general, however, ports in Africa, the former Soviet Union, and Eastern Europe have been slower to implement the required security measures. In a September 2004 bulletin, the U.S. Coast Guard named 17 nations with noncompliant port facilities.<sup>45</sup> Vessels that have visited one of the listed countries during their last five port calls will be subject to increased port state control actions upon arrival in the United States, the Coast Guard says. International pressure for compliance will be strong toward these

lagging nations in the coming months. Nevertheless, U.S. importers should closely monitor the current and future compliance of foreign ports and vessels they use and divert trade as necessary. In addition to Coast Guard detention of suspect vessels, trade through noncompliant ports or noncompliant carriers also will increase container targeting risk and the likelihood of inspection.

### **Action Point #3: Adjust Inventory Management**

Always looming over world commerce is the prospect of a successful attack on intermodal trade and its effect on targeting and inspections. A worst-case scenario in which terrorists exploit a C-TPAT-member supply chain, a CSI port, and internationally compliant carriers could in one stroke discredit America's entire security regime. "Since no shipment will be able to be viewed as low-risk" after such an incident, says Stephen Flynn of the Council on Foreign Relations, "U.S. authorities will have to attempt to inspect all shipments while it scrambles to then put a credible, verifiable security regime in place. In the interim we could bring the U.S. economy and the entire international trade system to its knees."<sup>46</sup>

There is a simple inverse relationship between supply chain security and efficient trade—namely, the more we protect against worst-case scenarios like the one above, the slower trade becomes, while fast and loose trade translates into much higher probability of an attack. Each extreme brings its own risks of delays, stoppages, and costs to intermodal trade, but so does the gray area in between—the daily uncertainty under which most of us work today. Research indicates the uncertainty may be attributable, in part, to CBP's strategy of targeting and inspecting containers overseas instead of inside the United States.

For example, if CBP delays a container abroad before lading, the shipment may miss its departing vessel and have to wait days before the next opportunity to sail. Delays at U.S. ports, on the other hand, are usually less severe because containers receive prompt truck and train service. Although no formal studies have been done, says Aaron Lukas of the Cato Institute, there is evidence that lead times at some foreign ports have risen by three to four days, or 30 to 40 percent, to counteract this uncertainty and ensure on-time U.S. delivery.<sup>47</sup>

As world trade volumes balloon in the coming years, increased cargo inspections and backlogs will make such preventive medicine for supply chains commonplace. To maintain supply chain efficiency on anything remotely resembling a just-in-time basis, firms may need to reexamine every aspect of inventory and logistics management. These measures might include:



- Greater automation of order processing;
- Location of factories, distribution centers, and warehouses in areas more strategic for security and disaster mitigation;
- Responsibility for shipments much earlier in the supply chain;
- Improved asset visibility and tracking;
- A domestic "mission control" for monitoring and directing international logistics;
- Larger emergency stock levels; and
- Diversion of some supply to stateside sources, or at least the plan for such a diversion in a crisis.

To be sure, all such options carry a quantifiable cost that must be weighed against trade risks. Companies must constantly assess current container targeting risk, future targeting and inspection potential, and current and future world security tensions when managing inventory. Such assessments also should weigh the effects of any changes made to the 24-Hour Rule and the way CBP processes advance cargo data, as discussed below.

### **Action Point #4: Prepare for Earlier Shipment Data Reporting**

Given the rising tide of imports and the corresponding increase in manifests being filed in advance to an increasingly overwhelmed agency, will the 24-Hour Rule ever become, say, the "36-Hour Rule"? Most likely, yes.

We can project the increase in U.S. imports with virtual certainty. On the other hand, suitable funding and staffing for CBP targeting functions, port operations, and other security-related programs much past the current fiscal year is decidedly uncertain. Because intelligence, targeting, and inspection remain dependent on human effort, despite high-tech computing also at work, the question arises: Will CBP targeters and inspectors eventually be unable to

review all manifests and related data (and possibly new document types) a mere 24 hours before lading? If the answer is yes, the prospect of giving them more time—thus shifting the cost to industry—seems more likely than additional money from Congress.

Because ports overseas will not be able to accommodate such an increase in parked containers waiting for permission to load, as discussed earlier, it follows that carriers or other entities will have to file manifest data long before containers arrive at their port of lading. (In fact, this already can occur under the 24-Hour Rule, which does not stipulate that a container be present before a carrier transmits the manifest to CBP.) The farther in advance a carrier files before taking possession of a container, the greater the chance of inaccurate data and, therefore, less effective targeting.

For example, the sea carrier has no way to include in his advance filing any information on container tampering, suspect seals, or route diversions or delays on land. A required shift

beyond the 24-hour timeframe, however, would necessitate 1) that carriers have a more concrete way to verify a container's contents; 2) the filing of advance cargo data by entities other than carriers (an idea discussed below); or 3) multiple filings of data during a container's journey to give more of a real-time picture of its status. Regardless of when or how CBP receives the filed data, changes in advance filing would add lead time to supply chains, further increase the demand for greater supply chain visibility, and require investment in automation for other chain partners involved—all at a cost.

Although a change in the period of advance reporting would require businesses throughout supply chains to adapt, such a change could have a net positive effect on efficiency once containers made it to the port of lading. As suggested by Aaron Lukas of the Cato Institute, logistics experts contend that ports could better sort arriving containers if they had advance notice of which ones are likely to be scanned or inspected manually. "If Customs receives information about the contents of a container before that container arrives at the port, as opposed to 24 hours before loading on a ship, then they can send that container to what is more likely to be the correct staging area, avoiding costly repositioning delays," Lukas says.<sup>48</sup>

And while the extension of the 24-Hour Rule may be

years into the future, it would be wise for U.S. importers and their supply chain partners to consider changes on the way. Building a flexible approach to advance filing and lead times into supply chain management today will surely reduce disruption and costs when CBP enacts a rule change down the road. It also will prepare firms for changes in the recipient of filed data, in the case of a new international targeting regime under the WCO or a similar entity.

### Action Point #5: Prepare for Broader Reporting Requirements

It is no secret, as discussed earlier in this report, that vessel manifest data does not present the most complete picture of a container's history prior to delivery to the carrier, who currently files the manifest under the 24-Hour Rule. The 14

data points required by the Rule, derived from a carrier's bills of lading, most often are not precise enough for the best possible targeting. For example, the information most needed by CBP is the identity of an importer's vendor, supplier, or manufac-

turer, though a carrier's bill of lading may often list a freight forwarder or other middle party as the shipper. This has presented a major problem to CBP from day one.

"Currently, the information CBP receives about the shipper is not helpful in making risk determinations," the agency says. "For example, identifying the shipper as a carrier, bank, or importer does not provide CBP with useful information."<sup>49</sup> CBP went so far as to change the definition of "shipper" in the Trade Act of 2002 to match its goal of learning the manufacturer's identity, but it had to suspend plans for enforcement of the change after an outcry from carriers. That suspension appears indefinite. Nevertheless, CBP warns that information given in the shipper field on manifests that is not useful in assessing risk will increase the likelihood of inspections. Carriers continue to insist that they should not be providing CBP with information they don't know or can't verify, all under the threat of penalty for inaccuracies.

So if—as the shipper controversy illustrates in part—manifest data filed by carriers is insufficient for the most precise targeting of high-risk cargo on a complex journey, what additional data is needed, and from whom?

A typical trade may involve the interaction of 25 different entities, use two or three different transportation modes, be handled at as many as 12 to 15 locations, and

generate 30 or more documents, including purchase orders, commercial invoices, shippers' letters of instruction, and certificates of origin.<sup>50</sup> A 2004 GAO report suggests that several such documents generated at stages throughout supply chains could be used in targeting.<sup>51</sup> Before that report, in 2003, U.S. senators from both parties on the Governmental Affairs Committee called on CBP to expand the number of documents it receives, including data collected at the time of purchase. "Purchase order data is historically more accurate and more detailed [than manifest data]," wrote Committee Chairman Susan Collins, R-Maine, and Ranking Member Joe Lieberman, D-Conn. "Import specialists and auditors already collect purchase order data to perform entry audits. If the information is already available to CBP when necessary, why should that data not be included earlier in the process to ensure a more accurate profile by ATS?"<sup>52</sup> The senators went on to suggest that additional documentation is necessary to target containers that have moved through multiple transshipment points prior to the port of lading, making it easier to catch terrorist attempts to hide a container's true origin or alter its contents. They cited a European Commission pilot program called Contraffice that tracks all of the ports of call for both containers and ships. "CBP could similarly minimize the vulnerability by requiring data detailing all ports of call for both the ship and all containers on it," they said.<sup>53</sup>

While it may be impractical, if not impossible, to require electronic filing of additional documents anytime soon, that day will come. Clearly, supply chain entities in addition to carriers will have to bear at least part of the reporting burden in the future. The Trade Act of 2002, in fact, states that, "In general, the requirement to provide particular information shall be imposed on the party most likely to have direct knowledge of that information."<sup>54</sup> To date, carriers have insisted that information about importers' vendors, suppliers, and manufacturers is best obtained from the importers themselves. In fact, importers provide this information to CBP in the merchandise entry process, though the data, of course, is not filed before vessel lading in time to be useful to ATS.<sup>55</sup> That may change. Shippers on foreign soil also may be responsible for filing information of which they possess the most direct knowledge. Such a requirement would require initial investment in infrastructure to convert and transmit documents in

electronic form, plus maintenance expenses to keep track as ACE and other government software platforms evolve over time. But even before the implementation stage will come an industry-wide debate over confidentiality. "Do shippers want their supplier and vendor lists given to carriers, and filed in the public manifest system?" asks Christopher Koch of the World Shipping Council.<sup>56</sup>

In addition to documentation of a container's contents and origin, the verification of secure practices in the stuffing, sealing, and land transportation of a container also should play a role in the targeting of suspicious cargo. While the issue of individual container security warrants a separate report of its own, it is worth noting

here that the prospect of "smart" containers and the related responsibilities placed on shippers will soon cross paths with advance reporting and targeting processes. Electronic sensors that can broadcast a container's location and security status via radio frequency or satellite are not a viable technology today, primarily due to the lack of accepted global standards and high start-up costs. Currently several CBP and industry programs (such as Operation Safe Commerce and Smart and Secure Tradelanes), as well as private manufacturers, are investigating solutions for smart container sealing and right-time tracking. Within individual supply chains, smart containers would undoubtedly enhance asset visibility and decrease cargo theft and pilferage. Once such containers become part of a worldwide infrastructure, however, CBP will want to monitor the data for its own reasons of security. Until that time, businesses should continue to follow and participate in smart container research programs to keep security-driven goals from outpacing practicality. Supply chain managers also should look ahead to the potential costs and implications of electronic seals, maintaining a network of seal readers, and ensuring the timely delivery of container data to CBP or other government agencies.



---

## Closing: Toward a More Organic Solution

Like so many other aspects of our lives, the way goods move into and out of the United States changed forever on September 11, 2001. In just over three years, a layered regulatory framework has descended upon intermodal trade with the dual goal of increased supply chain security and efficient commerce. Given a patient and growing terrorist threat, as well as projected increases in global trade volumes, that dual goal may prove impossible to CBP and other U.S. agencies if current security initiatives don't evolve to reflect a quickly changing world. Unfortunately, if history is our guide, sole reliance on government bureaucracy and congressional funding debates will make for a slow evolution—perhaps dangerously slow. While security initiatives must achieve the same prominence and untouchability as did our national defense during the Cold War, a slow, methodical buildup of a decades-long defense simply won't work in today's environment. The new terrorist enemy working in secret with unknown weapons and capabilities—and with surprise always on its side—is vastly different from our past superpower adversaries.

The prospect of general economic disaster and loss of life from a trade-related attack does place significant responsibility on government agencies for protection. And in the relatively short time since 9/11, CBP and its partners have done a commendable job in putting a system in place that offers one means for safeguarding trade. How effective the system is, however, no one knows for sure. And while it is one means for protecting commerce, it certainly isn't the only one and may not be the best. At the very least, as outlined in this report, companies must assume responsibility for internal security, then anticipate changes in the current federal system of targeting and inspection to mitigate delays and stay one step ahead of government mandates.

But industry can do better than simply following the federal lead and taking educated guesses about where it will head next. Industry can assume greater control.

Ensuring safe and efficient trade must involve quick, proactive management of risk. Who else but free-market business can best lead such an effort? While CBP will always play an integral role in protecting the nation at its points of entry, initiatives like ATS, CSI, and C-TPAT will have to go global and incorporate all customs agencies and all trading companies around the world if they are to achieve true protection of U.S. interests. Such a grassroots approach can best be directed by the system itself, through its members: the vast number of interconnected businesses around the globe. Like an organism that evolves to survive

a harsh new environment, the system—and not its regulators—will find the best way to flourish amid forces that want to destroy it. Market-driven new technologies and risk-managed security not only will provide greater protection. They also will create a network of intermodal trade that, even in the devoutly wished absence of global terrorism, works better than any system the world has ever known.

## Notes

1 Mark Gerencser, Jim Weinberg, and Don Vincent, *Port Security War Game: Implications for U.S. Supply Chains* (McLean, Va.: Booz Allen Hamilton, 2002), p. 3.

2 Michael E. O'Hanlon et al., *Protecting the American Homeland: A Preliminary Analysis* (Washington, D.C.: Brookings Institution Press, 2002), p. 7.

3 Testimony of Christopher Koch, Senate Committee on Commerce, Science, and Transportation, *The State of Maritime Security*, 108th Congress, March 24, 2004, p. 5.

4 Organisation for Economic Co-operation and Development, *Report on Container Transport Security Across Modes, Executive Summary and Conclusions* (Paris: OECD, 2004), p. 2.

5 While the Bioterrorism Act is a crucial part of protecting the nation's food supply, its enforcement is beyond the scope of this report. For more information, see [www.fda.gov/oc/bioterrorism/bioact.html](http://www.fda.gov/oc/bioterrorism/bioact.html).

6 The final 24-Hour Rule, officially titled "Presentation of Vessel Cargo Declaration to Customs Before Cargo Is Laden Aboard Vessel at Foreign Port for Transport to the United States," was published in the *Federal Register* in October 2002, with an effective date of December 2, 2002. For text of the final rule and CBP commentary, see *Federal Register* Vol. 67, No. 211 (October 31, 2002), pp. 66318-66333.

7 Government Accountability Office, *Container Security: Current Efforts to Detect Nuclear Materials, New Initiatives, and Challenges*, GAO-03-297T (Washington, D.C.: GAO, November 18, 2002), pp. 4-5.

8 In July 2004, the General Accounting Office changed its name to the Government Accountability Office.

9 Government Accountability Office, *Homeland Security: Summary of Challenges Faced in Targeting Ongoing Cargo Containers for Inspection*, GAO-04-557T (Washington, D.C.: GAO, March 31, 2004), p. 5, pp. 9-10.

10 Philippe Crist, *Security in Maritime Transport: Risk Factors and Economic Impact* (Paris: Organisation for Economic Co-operation and Development, 2003), p. 57.

11 The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (Washington, D.C.: U.S. Government Printing Office, 2004), p. 391.

12 Take, for example, the overwhelming attention paid to aviation security only after 9/11, or the overnight surge of interest in rail security following the March 2004 train bombings in Madrid. In the days following the train bombings, Congress drafted the Rail Security Act of 2004 and proposed expenditures of more than \$1 billion on U.S. rail security.

13 Testimony of Noel Cunningham (director of Operations and Emergency Management, Port of Los Angeles, speaking for the American Association of Port Authorities), House Subcommittee on Coast Guard and Maritime Transportation, Transportation and Infrastructure Committee, 108th Congress, June 9, 2004, p. 2.

14 Koch, p. 3.

15 Testimony of Richard Stana (director, Homeland Security and Justice, U.S. Government Accountability Office), House Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, *Port Security: A Review of the Bureau of Customs and Border Protection's Targeting and Inspection Program for Sea Cargo*, 108th Congress, December 16, 2003, p. 12.

16 Port of Long Beach, "Terminals Unveil 'Pier Pass' Program to Shift More Truck Activity to Off-Hours," [www.polb.com](http://www.polb.com), August 23, 2004, p. 1.

17 *Federal Register*, Vol. 68, No. 204 (October 22, 2003), p. 60465.

18 Kurt Nagle to Harold Rogers, chairman of the House Homeland Security Subcommittee, and Martin Olav Sabo, ranking member of the House Homeland Security Subcommittee, part of the Committee on Appropriations, May 26, 2004, p. 1. Available at [www.aapa-ports.org](http://www.aapa-ports.org).

19 The danger in leaving too much of the funding responsibility to the private sector, of course, is that the capital needed to make improvements fast enough to thwart imminent threats simply won't be available. For example, passenger aviation security received billions of new government spending, the lion's share of the required investment, immediately following 9/11, with positive results. One must wonder, however, how safe air travel would be today had airports and the cash-strapped airlines been required to shoulder most of the bill.

20 Testimony of Sen. John McCain (chairman), Senate Committee on Commerce, Science, and Transportation, *The State of Maritime Security*, 108th Congress, March 24, 2004, p. 1.

21 Consider, just as one example, the number of lawmakers who have called for the physical examination of *all* arriving containers—an impossible task.

22 Government Accountability Office, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors*, GAO-03-770 (Washington, D.C.: GAO, July 2003), p. 28.

23 Stephen Flynn (senior fellow, Council on Foreign Relations), "The Ongoing Neglect of Maritime Transportation," House Subcommittee on Coast Guard and Maritime Transportation, Committee on Transportation and Infrastructure, *Hearing on the 9/11 Commission Report and Maritime Transportation Security*, 108th Congress, August 25, 2004, p. 6.

24 GAO-03-770, p. 30.

25 Sandler, Travis & Rosenberg, P.A., "C-TPAT Surpasses 7,000 Members," *WorldTrade\Interactive*, [www.strtrade.com/wti](http://www.strtrade.com/wti), September 24, 2004, p. 1.

26 Senate Committee on Commerce, Science, and Transportation, *The State of Maritime Security*, 108th Congress, March 24, 2004, p. 1.

27 Testimony of James Carafano (senior research fellow, Heritage Foundation), Senate Committee on Commerce, Science, and Transportation, *The State of Maritime Security*, 108th Congress, March 24, 2004, p. 3.

28 Sandler, Travis & Rosenberg, P.A., "Bonner Seeks Global Cargo Security Standards," *WorldTrade\Interactive*, [www.strtrade.com/wti](http://www.strtrade.com/wti), September 24, 2004, p. 1.

29 GAO-03-770, p. 27.

30 Dennis Bryant (attorney, Holland & Knight LLP), "AMS, advance filing, SCAC, and ICB," *Haight's Maritime Items*,

[www.hklaw.com/maritimedevelop.asp](http://www.hklaw.com/maritimedevelop.asp), February 18, 2004, p. 1.

31 U.S. Customs and Border Protection, *ACE Fact Sheet*, [www.customs.gov](http://www.customs.gov).

32 Delays and cost overruns must be attributed, in part, to the unforeseen demands placed on the system by terrorism. See Peter Buxbaum, "CBP Deserves More Credit Than GAO Report Gives," *American Journal of Transportation*, [www.ajot.com](http://www.ajot.com), June 5, 2004.

33 Charles Bartoldus, director of the National Targeting Center, points out that ATS can detect anomalies in both accurate and inaccurate data. See House Subcommittee, *Port Security*, p. 3.

34 GAO-04-557T, pp. 9-10.

35 U.S. Customs and Border Protection, *Frequently Asked Questions: 24-Hour Advance Vessel Manifest Rule*, [www.customs.gov](http://www.customs.gov), p. 26.

36 Flynn, p. 7.

37 At present, carriers may apply for and receive an exemption to the 24-Hour Rule for specific break-bulk cargo that poses a low risk in the eyes of CBP.

38 The tests occurred in 2002 and 2003. See GAO-04-557T, p. 11. The embarrassing tests prompted a September 2004 report by the DHS Office of Inspector General, which made specific recommendations for improvements to detection equipment and search protocols.

39 Testimony of Robert Bonner, Senate Committee on Commerce, Science, and Transportation, *Oversight of Transportation Security*, 108th Congress, September 9, 2003, p. 3.

40 Testimony of Edward Henderson (director of strategic planning and development, Philadelphia Regional Port Authority), House Subcommittee, *Port Security*, p. 2.

41 Paul Scott Abbott, "Kerry urges more inspections, increased offshore deterrence," *American Journal of Transportation*, [www.ajot.com](http://www.ajot.com), June 5, 2004.

42 U.S. Customs and Border Protection, *Frequently Asked Questions: 24-Hour Advance Vessel Manifest Rule*, [www.customs.gov](http://www.customs.gov), pp. 8-9.

43 U.S. Customs and Border Protection, *Container Security Initiative (CSI) Fact Sheet*, [www.cbp.gov](http://www.cbp.gov).

44 International Maritime Organization, "Security compliance shows continued improvement," [www.imo.org](http://www.imo.org), August 6, 2004, p. 1.

45 U.S. Coast Guard, "Port Security Advisory," September 9, 2004. The 17 nations identified in the advisory were Albania, Benin, Dem. Rep. of Congo, Equatorial Guinea, Guinea, Guinea-Bissau, Kiribati, Lebanon, Liberia, Madagascar, Mozambique, Nauru, Nigeria, Serbia and Montenegro, Sierra Leone, Solomon Islands, and Suriname.

46 Flynn, p. 7.

47 Lukas expands on the uncertainty idea first suggested by Chip White of the Georgia Institute of Technology. See Lukas, p. 12.

48 Lukas, p. 13.

49 U.S. Customs and Border Protection, *Frequently Asked Questions: 24-Hour Advance Vessel Manifest Rule*, [www.customs.gov](http://www.customs.gov), p. 25.

50 Crist, p. 24.

51 GAO-04-557T, p. 22.

52 Sen. Susan Collins and Sen. Joseph Lieberman to Asa Hutchinson, under secretary for Border and Transportation Security, Department of Homeland Security, October 28, 2003, p. 3. Available at <http://govt-aff.senate.gov>.

53 Collins and Lieberman, p. 3.

54 *U.S. Statues* 116 (2002): p. 982.

55 Koch, p. 3.

56 Koch, p. 3.