April 8, 2004 No. 27

Protection without Protectionism

Reconciling Trade and Homeland Security

by Aaron Lukas

Executive Summary

For decades, criminals have used cargo containers, trucks, and train cars to illegally bring narcotics, weapons, and people across U.S. borders. The vulnerabilities that smugglers exploit are also available to terrorists.

The attacks on the USS Cole in the port of Yemen in 2000 and the French oil tanker Limburg in 2002 illustrate the direct threat that terrorism poses to seagoing vessels. Another prospect is that ships, trains, or trucks could be used in conventional suicide attacks, much like hijacked airliners were used on 9/11. A cargo ship or train car could also be exploded or sunk in a port or rail yard, damaging the facility and blocking commercial traffic. The worst-case scenario would involve a weapon of mass destruction entering the country via trade channels. Even a relatively modest nuclear weapon detonated in a major seaport would kill between 500,000 and 1 million people, directly destroy up to $500 billion worth of property, cause losses due to trade disruption of $100 to $200 billion, and impose further indirect costs of up to $1.2 trillion.

The Department of Homeland Security has begun implementing programs and procedures designed to safeguard the transportation and supply chains. States, shippers, port authorities, exporters, manufacturers, and foreign governments all have important roles to play in that effort. Federal rules and regulations are necessary but should be as open-ended as possible. They should set security goals and verify how well the private sector meets them, rarely mandating specific technologies or processes. Securing the trading system against terrorism is a regrettable but real cost of doing business internationally, and consumers and companies should not be insulated from those costs.

The challenge for U.S. policymakers is to improve security while minimizing the loss of liberty and the benefits of economic openness. The task is made more difficult by domestic interests that press for measures that unfairly hinder their foreign competitors without appreciably improving U.S. security.

Aaron Lukas, formerly chief speechwriter and strategic adviser for the Office of the U.S. Trade Representative, is an analyst at the Cato Institute's Center for Trade Policy Studies.

CATO INSTITUTE

The free movement of goods across U.S. borders is a key pillar of the nation's prosperity.

Introduction

The September 11, 2001, terrorist attacks on New York and Washington have spurred dramatic changes in how the United States protects itself. Most notably, the Homeland Security Act of 2002 created the Department of Homeland Security in the largest reorganization of the federal government since the creation of the Department of Defense in 1947. DHS encompasses 22 previously disparate domestic agencies and is charged with analyzing threats and intelligence, guarding America's borders and airports, protecting critical infrastructure, and coordinating the efforts of other agencies—federal, state, and local—in the fight against terrorism.

News reports have tended to focus on DHS activities that directly affect travelers. Initiatives such as an expanded air marshal program, tightened airport security, and the fingerprinting of foreign visitors have been well covered in the popular press. A less appreciated but more challenging task is reducing the risk of a terror attack carried out via the mechanisms of trade.

Despite some protectionist lapses in specific sectors,[1] the United States has, by and large, a very open economy. Indeed, the United States is the world's largest single exporter and importer. Every day, millions of tons of cargo worth billions of dollars enter the country across 7,514 miles of border and 95,000 miles of shoreline. Shipments arrive by land, sea, and air into some 350 commercial ports of entry. Ninety percent of these goods (by volume) are shipped in cargo containers—opaque metal boxes about the size of railroad cars—approximately 21,000 of which enter the United States each day.[2]

The free movement of goods across U.S. borders is a key pillar of the nation's prosperity. Unfortunately, our dynamic trading system is also a conduit that terrorists may exploit.

For decades criminals have used cargo containers, trucks, and train cars to illegally bring narcotics, weapons, and people across U.S. borders. The vulnerabilities that smugglers exploit are also available to terrorists—with a potential for harm that far exceeds garden-variety crime. U.S. intelligence has reported, for example, that Osama bin Laden's al Qaeda organization owns and operates at least 15 cargo freighters worldwide that could be used in direct attacks or in support of other operations.[3] In fact, terrorists have been open about their intentions to attack commercial targets and use the global trading network as a weapon. "We are attempting to expand the frontlines," said Abu Laith Al-Libi, an al Qaeda spokesman. "It will be a war of killings, a war against businesses, which will hit the enemy where he does not expect."[4] Meanwhile, in Asia, the Liberation Tigers of Tamil have attacked maritime targets directly and deployed waterborne mines.[5]

There are several ways that terrorists could exploit the trading network to achieve murderous ends. The attacks on the USS *Cole* in the port of Yemen in 2000 and the French oil tanker *Limburg* in 2002 illustrate the direct threat that terrorism poses to seagoing vessels. Another prospect is that ships, trains, or trucks could be used in conventional suicide attacks, much like hijacked airliners were used on 9/11. A cargo ship—perhaps one carrying a flammable cargo, such as liquid natural gas—could also be exploded or sunk in a port, damaging the facility and blocking commercial traffic. The same result could be achieved by detonating a tractor trailer at a U.S. land-border crossing. At a recent terrorism conference in London, maritime security experts predicted a "spectacular" attack of this sort sometime in the near future.[6]

The movement of goods also offers an avenue for the terrorists themselves to circumvent border and immigration controls. Terrorists might enter the country as crew members on a ship, for example. There are approximately 1.2 million officers and crewmen manning the world's merchant fleets, a significant portion of whom work on commercial trading vessels.[7] Many of these people have not undergone background checks of any kind—a reality underscored by the fact that crewmen are sometimes complicit in cases of piracy. Forged seafarer certificates and identity documents are also readily available on the black market. It does not take

much foresight to predict that terrorists will seek to exploit such lapses.

Terrorists might potentially stow away inside a cargo container. Although there has been no confirmation of a terrorist successfully entering the United States in this manner, botched attempts have been documented. The 43-year-old Egyptian Rizk Amid Farid, for example, attempted to enter Canada in a shipping container that had been outfitted with a bed and toilet. Farid—who had trained as an airline mechanic—was discovered in the Italian port of Gioia Tauro with two cellular phones, a satellite phone, a computer, cameras, and various forms of forged identifications. The stowaway would likely have gone undetected if he had not been trying to widen the container's ventilation holes and made noise that was overheard by port workers.[8]

The direst threat we face is the use of trade as a conduit for weapons of mass destruction (WMDs). Cargo containers, rail cars, and tractor trailers are large enough to transport chemical, biological, or nuclear weapons. In the case of the maritime trade, a weaponized container would not require anyone to meet it upon arrival because it could be detonated by remote signal or timer as it sat in a U.S. port or rail yard. Even a relatively modest attack delivered in this fashion could be massively costly for the United States. The consulting firm Booz Allen Hamilton ran a strategic simulation in which "dirty bombs"—devices that use conventional explosives to disperse radioactive material—were discovered in cargo containers at three U.S. ports. The estimated cost to the economy from the resulting disruption of trade was $58 billion.[9]

At the far end of the spectrum would be the detonation of a full-scale nuclear device inside a cargo container. Even if the container were restricted to its port of entry, many container storage facilities and rail yards in the United States sit in the center of densely populated areas. A nuclear detonation in a port such as Los Angeles, Houston, or Baltimore could result in massive casualities. One study estimated that a relatively modest (10- to 20-kiloton) weapon detonated in a major seaport would kill between 500,000 and 1 million people, directly destroy up to $500 billion worth of property, cause losses due to trade disruption of $100 to $200 billion, and impose further indirect costs of up to $1.2 trillion.[10]

Securing Trade against Terrorism

The potentially catastrophic consequences of terrorist misuse of the trading system mean that its security must be a U.S. priority. And Washington has taken steps to address the threat. Since the attacks of 2001, the number of inward-bound cargo containers inspected by Customs (across all modes of transportation) has risen by nearly two-thirds, from 7.6 percent to 12.1 percent of the total. For sea containers, the increase has been from 2 percent to 5.2 percent.[11] In addition, DHS has begun implementing new programs and procedures—the 24-hour rule, the Custom-Trade Partnership against Terrorism, the Container Security Initiative, Operation Safe Commerce, and others—designed to safeguard the transportation and supply chains. The goal, according to policymakers, is to "push the border outward" by decreasing the chances of terrorist infiltration of trade networks before goods ever arrive in the United States. Robert Bonner, commissioner of the new U.S. Customs and Border Patrol, put it this way:

> We can no longer afford to think of 'the border' merely as a physical line separating one nation from another. We must also now think of it in terms of the actions we can undertake with private industry and with our foreign partners to prescreen people and goods before they reach the U.S. The ultimate aims of 'pushing the border outward' are to allow U.S. Customs more time to react to potential threats—to stop threats before they reach us—and to expedite the flow of low-risk commerce across our borders. [12]

It is significant that Commissioner Bonner takes care to mention private industry and for-

The direst threat we face is the use of trade as a conduit for weapons of mass destruction.

eign partners. Many countries, jurisdictions, entities, and individuals have a stake in the trading system, so it is neither possible nor desirable for the U.S. federal government to bear the burden of security alone. States, shippers, port authorities, exporters, manufacturers, and foreign governments all have important roles to play. The large number of players in this game also raises questions about who benefits most from improved security and who should fund it. Although governments have some responsibility to provide security, ports, shippers, exporters, consumers, and other stakeholders often reap many of the benefits. In some cases, then, these nonfederal actors may be the most appropriate source of funds.

Between 1960 and 2000, the value of America's exports plus imports grew from about 8 percent of U.S. gross domestic product (GDP) to nearly 26 percent.[13] Trade is the lifeblood of the U.S. economy and cannot be curtailed without greatly restricting U.S. standards of living. Falling transportation costs and business innovations such as just-in-time inventory and disaggregated production have further elevated the role of trade in maintaining America's prosperity. Factories that decades ago built cars from raw materials now assemble parts made all over the globe. Such economic interconnectedness means we can make more, better products with fewer resources. Yet it also means that even a brief interruption of international commerce can be enormously costly. Following the 9/11 attacks, for example, the Ford Motor Company was forced to idle several of its assembly lines as trucks loaded with parts were delayed at the Mexican and Canadian borders. For longer interruptions of international trade, such as the 2002 shutdown of U.S. West Coast ports during a longshoremen's strike, the hit to America's economy can be measured in the billions of dollars.

It is neither possible nor desirable for the U.S. federal government to bear the burden of security alone.

Balancing Costs and Benefits

Protecting America's economy and people from assaults on trade is a necessary venture. Yet there are limits to what can be done. Security, like other goods, is subject to the law of diminishing returns. The United States could conceivably seal its borders and cease trading with other nations. Halting all trade, now and forever, would eliminate the threat of a bomb in a cargo container. But exchanging the possibility of a terror attack for the certainty of a poorer nation—and thereby advancing an end that America's enemies seek—would not be a wise course of action. We must instead recognize the inevitable tradeoffs between security and efficiency and seek to balance costs with benefits. Americans have the right to do business with anyone they choose—and that right should only be restricted in extraordinary circumstances.

In brief, the challenge for U.S. policymakers is to improve security while minimizing the loss of liberty and the benefits of economic openness. The truth is that the United States will never be completely secure. Opportunities to exploit the trading system for nefarious ends will always exist.

Although risk cannot be eliminated, it can be managed. A layered system can have safeguards that build upon one another at all stages of trade—from packing, to ports, to shipping, to border controls, to personnel checks. No single component of the system will be infallible, but taken together, overlapping precautions make a major tragedy unlikely. In the event that defenses fail and a terror attack on (or delivered via) the institutions of global trade occurs, robust layered security can minimize disruption by giving officials the confidence to respond without shutting down commerce altogether.

The optimal balance between security and openness is difficult to determine even in the best of times. Achieving that balance is even more difficult because of the temptation for domestic interests to press for measures that unfairly hinder their foreign competitors without appreciably improving U.S. security. Such protectionism masquerading as homeland defense is more than a theoretical possibility. Legislation has been introduced in Congress, for example, that would require all inbound ships to have their cargos screened at an offshore location before landing in the United

States. Such draconian approaches would hobble the U.S. economy while providing little additional security.

This paper begins with a framework for thinking about how the burdens of securing trade should be apportioned. Next it examines some ongoing U.S. and global initiatives. It concludes with discussions of new technologies and the dangers of justifying protectionism under the guise of security. Although the focus here is on trade—threats centered on how commercial goods enter the United States—it is important to remember that this is only one aspect of border security. In 2002, for instance, Customs conducted some 453 million inspections of property carried by individuals into the country.[14] The challenge of securing the United States against the threat posed by foreign visitors is as daunting as that posed by cargo shipments. Programs such as the recently launched US-VISIT—which collects biometric information on temporary visa holders and verifies that they leave the country on time—are a large part of the DHS portfolio; they are, however, beyond the scope of this report. In sum, U.S. efforts to make global trade more secure should be viewed as just one part of a larger homeland defense strategy.

A Framework for Evaluating Trade-Security Initiatives

Because each American benefits equally from the existence of the U.S. armed forces regardless of how much tax he pays, there is an incentive to free ride on the security purchased by fellow citizens. Defense is, in other words, one of the very few genuine examples of a "public good"—or in this case, a public service—that probably would not be produced in sufficient quantities if people individually chose how much they wished to pay for it. As the economist David Friedman has put it, "The problem with public goods is not that one person pays for what someone else gets, but that nobody pays and nobody gets."[15] That dynamic is what led to a national defense system that is funded primarily through taxation.

There are differences, however, between securing the nation and securing trade. Trade is carried on by private actors pursuing profit. And although the federal government is charged with protecting the United States generally, it is not incumbent on Washington to safeguard every ship, train, truck, and factory from all manner of conceivable harm. Just as "national defense" does not entitle every homeowner to a federally funded burglar alarm, it does not relieve private businesses from the responsibility of providing much of their own security. Alarms, security guards, locks, and insurance are all security measures most people think should be funded privately because the benefits flow mostly to those who purchase them. When such precautions fail, local police and courts are usually expected to find and punish those who have stolen private property or taken lives. Similarly, we can reasonably expect private actors in international trade to pay for their own security in many cases—backed and aided, of course, by the efforts of law enforcement, intelligence agencies, and the military.

The concept of liability is also important when considering how the burden of security should be apportioned. One reason businesses are willing to pay to safeguard their property is that they can often be held responsible for its misuse. Imagine a gun shop that decided not to "waste" money on door locks. It is likely that the foolish proprietors of such a business would face multiple lawsuits if thieves stole weapons from them that were then used to commit crimes. The law expects that businesses should take reasonable and prudent precautions against their property being used to harm others. Although litigiousness can be and has been taken too far, the basic concept is sound: Holding businesses to a standard of responsibility gives them an incentive to behave sensibly without the need for rules that detail every action that they should take.

In the area of security, there are many reasons to prefer liability to regulation or direct government provision. Flexibility is one advantage. Companies face varying degrees of threats, and individual businesses are often in the best position to know where their weak-

Protectionism masquerading as homeland defense is more than a theoretical possibility.

Just as "national defense" does not entitle every homeowner to a federally funded burglar alarm, it does not relieve private businesses from the responsibility of providing much of their own security.

nesses lie. Uniform regulation may lead to too much security in some sectors and not enough in others. Relying on incentives rather than regulation also guards against the real possibility that regulators will be "captured" by those they supervise. The history of regulation is littered with rules designed to stifle competitors instead of enhance public welfare. Finally, regulation can lead to an unjust distribution of costs, with taxpayers or companies that face few threats subsidizing the security of firms that engage in riskier behavior.

However, civil liability does have limits. Where costs would be extraordinarily high, for example, a company could never hope to compensate damaged third parties. Or when damage could be widespread, such as when negligence would lead to mass casualties, then regulation, even when less than optimally efficient, might be prudent. Few people would feel comfortable with the idea that a nuclear plant, for example, should be able to operate in whatever manner its owners wish so long as they are held liable for any mishaps. Indeed, in cases where potential negative externalities—damage to third parties—is extremely large, no compensation would be possible even if society were willing to tolerate the risk.

International trade is a field where it is difficult to establish the proper mix of incentives, liability, regulation, and direct government provision of security. However, faced with the nightmare scenario of terrorists using the trading system to deliver a WMD that could kill millions of civilians, most people will probably conclude that the high potential cost in terms of innocent human life is a significant externality—one that fully justifies government intervention in the market for cargo security.

So if we accept that government will play a leading role, what principles should guide policymakers in thinking about trade security?

First, as in all public policy endeavors, the danger of "government failure" must be recognized. Just because the free market may yield too little of a public good does not mean that government will do any better. As any trip to the department of motor vehicles will attest, government agencies are often inefficient. Regulators do not always act in the public interest. Politicians will seek support from companies that provide security technologies in exchange for favorable legislation. And bureaucracy can be inflexible, wasteful, and overly conservative in its approach to solving problems. As a rule, then, private actors should carry out day-to-day security responsibilities, and whenever feasible, costs should be passed on to consumers, not taxpayers.

Second, where rules and regulations are necessary, they should be as open-ended as possible. In such cases, policymakers should set security goals and verify how well companies meet them, not mandate specific technologies or processes. Positive incentives should be considered to encourage companies to be vigilant and to guard against regulations becoming a best practices ceiling, rather than a floor. For example, instead of merely mandating specific intrusion-detection technology for cargo containers, DHS could offer bounties to companies that uncover terrorists or weapons. When the government is seeking to develop new security technologies, it should consider offering bonuses and contracts to the first company that can develop the desired product or meet the specified goal—avoiding "seed money" research grants that are too often awarded on the basis of political criteria.[16]

Third, policymakers should be aware that securing the trading system against terrorism is a regrettable but real cost of doing business internationally. The prices of imported goods should reflect those costs. The United States benefits from imports when their price and/or quality advantage outweighs their total cost, including the cost of transportation and security. Expansive taxpayer subsidies for commercial security may distort economic decisions and prompt companies to make unwise investments. At the same time, however, it is important that the cost of new security measures be justified by their safety benefits. "Security" should never become an excuse for protectionism.

America's ports also deserve scrutiny in terms of subsidies and ownership. Public port authorities own all major U.S. seaports and operate many of them. (A 1990 report by the American

Association of Port Authorities showed that 30 percent of the 66 port authorities surveyed were operating at a loss.) As a study by the Reason Foundation reported, government-owned and -operated ports face many problems. In the post-9/11 environment, streamlined port operations will be critical to offset security-driven efficiency losses. Yet publicly owned and operated ports are regularly subjected to political interference and have weakened incentives to operate efficiently because they are insulated from commercial competitive pressures. Public ports have also been known to soak up funds from local governments and drag down local economies. Conversely, relatively efficient public ports are often targeted by local governments that want to siphon off "surplus" funds.[17]

Finally, security policy should always be developed with an eye toward the U.S. Constitution. Reducing the risk of terrorist attack on or through the trading system is an important objective, but it must be achieved within a framework of law that protects the civil liberties and privacy of U.S. citizens.

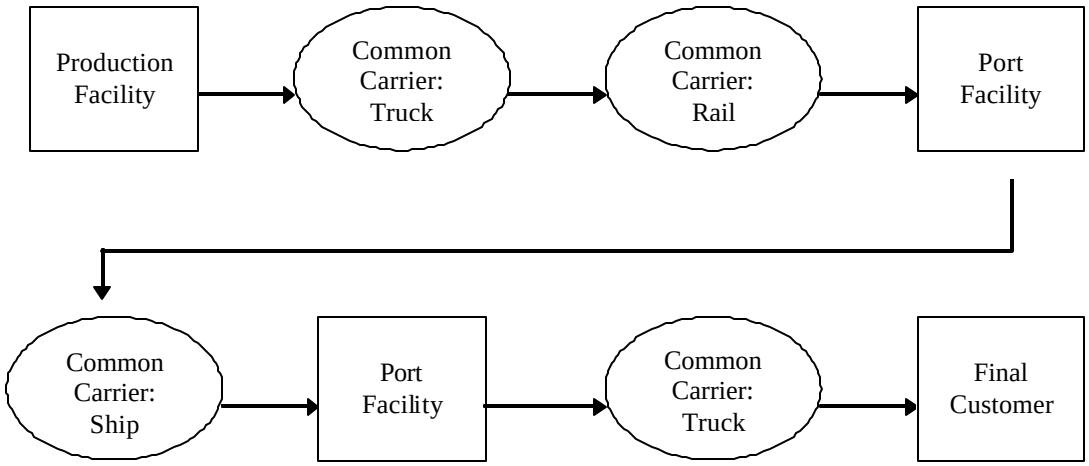
The Complex World of Cargo Shipping

Even if federal resources were unlimited, the task of making the global trading system more secure would be daunting. To fully appreciate the challenge, consider the following hypothetical account of the journey of computer memory chips manufactured in China.

XYZ Enterprises fabricates RAM chips in its production facility in central China. It packs the chips into boxes and then turns them over to a private freight forwarder that combines the boxes with freight from other companies and loads them into a steel shipping container. The forwarder transports the container to a rail yard where the container is loaded onto a train run by the Chinese government. The train takes the container to a port in Hong Kong, where it is unloaded onto a storage yard. The RAM chips sit at the port for three days before being loaded onto a Panamanian-flagged ship bound for Los Angeles. A multinational crew mans the ship, with most sailors coming from countries in the Asia-Pacific, especially Indonesia. While en route to Los Angeles, the ship makes a stop in the Philippines to pick up cargo and change crew. Upon arrival in the United States, the container of RAM chips is unloaded and placed on a truck owned by an American company. Finally, the container is driven to the warehouse of a retail distributor in San Jose where the customer takes delivery of the product.

In this example, as Figure 1 illustrates, a single shipment of computer chips changes hands at least six times before reaching the final buyer.

Figure 1
Global Shipments Change Hands Often



Securing the trading system against terrorism is a regrettable but real cost of doing business internationally.

Even if federal resources were unlimited, the task of making the global trading system more secure would be daunting.

The manufacturer, the freight forwarder, the railroad, the port authority in Hong Kong, the shipping company, the Port of Manila, the Port of Los Angeles, and an American trucking company all have some control over it at different stages. This scenario is not unusual; indeed, many shipments follow paths far more convoluted than the one described above. According to the Organization for Economic Co-operation and Development, the typical door-to-door journey using a shipping container will involve the interaction of about 25 different actors, generate 30–40 documents, use 2–3 different transportation modes, and be handled at 12 to 15 physical locations.[18]

There are many points during this imaginary journey where the shipment could be susceptible to terrorist infiltration or tampering: at the manufacturer; during or before packing; during movement by rail, especially when the train is stationary at a switching station or side track; at the port in Hong Kong; during the voyage by sea; and finally, at the port in Los Angeles before clearing customs. In addition, if the container had landed in Canada or Mexico and then traveled to the United States by ground—as many cargos do—that would create more points of vulnerability. The fact that thieves regularly violate the integrity of the cargo chain—with worldwide thefts estimated at $30–50 billion per year by the OECD—illustrates the leakiness of today's international trade environment.[19]

The ideal security system would offer what experts call "Total Asset Visibility and Authentication"—integrated procedures and technologies that safeguard cargos at all stages of transport. Total Asset Visibility and Authentication would require (1) loading of shipments in a secure facility, by authenticated personnel; (2) verification of the contents of a shipment; (3) security in transit; (4) transmitting the content and manifest information to Customs and stakeholders upon loading; (5) the ability to identify container tampering; and (6) a way for Customs to provide verification of a container's contents and integrity in a nonintrusive manner at the point of entry.[20]

Such a system is not without precedent. The Department of Defense's Total Asset Visibility Network (TAV) uses radio frequency tags with full electronic container manifests attached to containers, wireless tag readers located at checkpoints around the world, and a computerized system to track and monitor the status of the containers. The TAV system uses checkpoints at more than 400 locations in 36 countries—military and commercial seaports, airports, rail terminals, and military bases—to track the movement of some 250,000 conveyances.[21]

Although the U.S. government is exploring the move toward a TAV system for private commerce, the current programs have not moved much beyond demonstration and testing. This does not mean that security officials have been derelict. Securing the trading system is an enormously complex and expensive task—one that could not have been reasonably completed in the two years since the attacks on New York and Washington. The approach has been to create multiple programs that focus on different components of the trading system, from loading to delivery, for several modes of transport. Those programs will naturally take time to implement.

There are many potential ways to assess U.S. initiatives to date, but six questions seem especially relevant: First, do the major U.S. efforts to improve trade security address the areas of vulnerability? Second, how effective will they be in reducing risk? (In other words, are there obvious holes that can be exploited by terrorists?) Third, are programs sufficiently open-ended that they will be able to incorporate new technologies down the road? Fourth, are current programs likely to be prohibitively expensive? Fifth, what are the major hurdles to full implementation of each particular program? And finally, is the burden of security being fairly distributed among the major trade players?

Survey of Major Trade-Security Programs

> Today we are more vigilant and more secure and better prepared as a nation than ever before.[22]
>
> – Tom Ridge, Secretary of the Department of Homeland Security

The United States is pursuing a multifaceted approach to trade security. While the Department of Homeland Security has taken the lead, many other agencies, state and local governments, and private actors are also active on this front. DHS alone has dozens of initiatives of varying scope and ambition. The following list is thus not comprehensive, but is intended to highlight major efforts.

The Container Security Initiative and the 24-Hour Rule

Cargo containers are at the heart of the transport chain. In fact, some 90 percent of international trade, across all modes of transportation, moves inside these standardized steel boxes—although most containers entering the United States arrive by sea.[23] Containerized shipping is highly efficient because goods are protected from the rigors of transport, can be moved quickly from road to rail to ship using the same equipment, and can be stacked vertically to minimize space requirements. The widespread use of containers has helped cut shipping costs—and, by extension, the prices consumers pay for goods—dramatically over the past half century.

Long before combating terrorism moved to the top of the global agenda, authorities were aware that shipping containers were exploitable for criminal purposes. The United States alone reported 950 seizures of cocaine, marijuana, and heroin in commercial ocean cargo shipments and vessels from 1996 to 1998, representing some 223,000 kilograms of drugs.[24] In fact, the flow of contraband that enters the United States by sea is estimated to be greater than that which enters via the U.S. border with Mexico.[25] Piracy also continues to be a serious problem, with the International Chamber of Commerce reporting that 335 attacks on commercial vessels took place in 2001.[26] Piracy can range from stolen cargo to kidnapping to the theft of an entire vessel.

The U.S. agency bearing primary responsibility for cargo container security is Customs and Border Patrol. CBP is an arm of DHS that was created by combining several previously existing agencies: Border Protection, the Immigration and Naturalization Service, Agriculture Inspection, and the U.S. Customs Service. The Container Security Initiative, launched in January 2002, is at the center of the federal government's efforts to make the sea trade more secure; to "push the border outward" by countering terrorist threats before they reach U.S. shores. According to DHS, it is the only formal federally administered program in operation today designed to detect WMDs and to deter terrorists from exploiting the vulnerabilities of containerized cargo.[27]

The CSI has four stated goals:

1. To establish international security criteria for identifying high-risk cargo that may contain terrorists or terrorist weapons.
2. To prescreen high-risk containers at the port of shipment, before they are shipped to the United States.
3. To maximize the use of detection technology, such as X-rays and radiation and chemical detection sensors, to prescreen high-risk containers.
4. To develop and deploy smart and secure boxes with electronic seals and sensors to ensure cargo integrity, especially after prescreening.[28]

In short, CSI seeks to integrate five components—U.S. inspectors in foreign ports, intelligence from outside the shipping community, advance knowledge of container contents, better passive screening technologies, and "smarter" cargo containers—to reduce the risk of terrorism.

One of the most controversial parts of the CSI is the stationing of U.S. Customs teams in foreign ports. The U.S. teams are tasked with helping the local port authority identify and target high-risk containers for pre-screening before they are shipped to the United States. It should be noted that U.S. Customs officers do not conduct inspections themselves; instead, they observe inspections conducted by local port officials.

Containers that are screened prior to loading and those that are designated "low risk" do not face any additional scrutiny when they reach the United States unless information sur-

The ideal security system would offer integrated procedures and technologies that safeguard cargoes at all stages of transport.

The United States is pursuing a multifaceted approach to trade security.

faces in transit that alters the original risk assessment. Customs officers are stationed on a reciprocal basis, meaning that CSI countries are invited to send their own inspectors to U.S. facilities. The biggest benefit of participating, however, would come in the case of a crisis, when all shipments might be turned away except those originating from CSI ports.

The initial implementation of CSI has focused on securing the participation of the world's 20 largest foreign ports. Cumulatively, these facilities account for over 70 percent of inbound container traffic to the United States.[29] Ports currently participating in the CSI are Vancouver, Montreal, and Halifax (Canada); Felixstowe (UK); Le Havre (France); Antwerp (Belgium); Rotterdam (Netherlands); Gotëborg (Sweden); Hamburg and Bremerhaven (Germany); Genoa and Le Spezia (Italy); Hong Kong (China); Singapore; Yokohama (Japan); Busan (South Korea); and Pretoria (South Africa). Ten additional ports are slated to begin participation soon.[30]

Eventually, the goal is to have all ports that handle U.S.-bound traffic enrolled in CSI. CBP lists the following criteria for potential new CSI ports:[31]

- Seaport must have regular, direct, and substantial container traffic bound for the United States.
- U.S. Customs must be able to inspect cargo originating, transiting, exiting or being transshipped through a country.
- Nonintrusive inspection equipment (gamma or X-ray) and radiation detection equipment must be available for use at or near the potential CSI port.
- Port must establish an automated risk management system.
- Port authorities must share critical data, intelligence, and risk management information with U.S. CBP.
- Port must commit a thorough security assessment and commit to resolving port infrastructure vulnerabilities.
- Port must maintain integrity programs and identify and combat breaches in integrity.

It is difficult to pass judgment on CSI because the program is still relatively new. Success will ultimately depend on several unknowns: First, the extent to which CSI's reporting requirements help Customs effectively target high-risk containers for greater scrutiny; second, whether or not a majority of foreign ports can be persuaded to participate; and third, how widely and effectively the intrusion-detection and tracking technologies called for by the program can be put into action.

Since the CSI was announced two years ago, the Bush administration has made undeniable progress in implementing it. One measure of progress is that U.S. Customs claims that it has more than doubled the number of containers it physically inspects, from about 2 to 5 percent. New scanning and detection equipment also continues to be deployed.

Another step forward has been implementation of a "24-hour rule" that requires carriers to file detailed cargo manifests with CBP a full day before a U.S.-bound container is loaded onto a vessel in a foreign port. The idea is to give Customs the information and time to target shipments deemed to be "high risk," such as those from companies with suspected ties to terrorist organizations. Information collected under the 24-hour rule is fed to Customs' Automated Manifest System—the computerized federal data management system that ranks cargo information on a set of classified risk criteria. In conjunction with AMS, the 24-hour rule appears to have substantially improved the information that Customs has on the contents of shipments to the United States. In addition to providing information earlier, shippers are required to transmit better information about a shipment than was previously common.[32] Generic descriptions of a cargo container's contents—such as "Freight of all Kinds" and "General Merchandise"—are no longer accepted.

Over the 24-hour rule's first week, CBP reported reviewing more than 142,000 bills of lading.[33] Noncompliant shippers and Non-Vessel Operating Common Carriers have faced penalties. Current data are unavailable, but from February through June 2003, CBP reviewed

1.65 million bills, targeted 141,000 shipments for additional screening, and issued 97 "No-Load" directives.[34] (A "No-Load" directive means that U.S. Customs has instructed an ocean shipping line not to load a container at a foreign port for delivery to the United States.) Most of the "No-Load" orders were prompted by incomplete cargo descriptions. Some also involved inadequate consignee information.

Another way to measure CSI's progress is the number of foreign ports that have chosen to participate—currently 19 facilities representing nearly 70 percent of inbound U.S. container traffic (out of a total 20 points that were initially targeted).[35] Although the number of foreign ports that participate in CSI has been rising, America's trading partners have not offered an unqualified embrace of this program. In general, their objections have fallen into three categories: sovereignty, trade diversion, and expense.

Sovereignty. Some nations—particularly those in Asia—are concerned about CSI's impact on national sovereignty and are anxious to avoid appearing subservient to the "American Empire." As an official from the Singapore Ministry of Defense notes: "Worries linger that CSI could become a back door for unbridled external interference in domestic jurisdiction and enforcement regimes over port operations."[36] Other nations, most notably Australia, have expressed concerns that CSI is too U.S.-centric and could undermine parallel international efforts. As a report by the Department of the Parliamentary Library—Australia's equivalent of the Congressional Research Service—noted, "The U.S. Customs CSI might just have preempted what is perhaps a more coordinated approach to improving the security of commercial shipping worldwide."[37] (Australia has taken a "wait and see" approach to CSI).

Trade Diversion. European governments in particular have raised concerns about potential port discrimination under CSI. In June 2003, representatives of U.S. Customs and Border Protection met with members of the European Commission and both sides expressed a willingness to continue cooperating on maritime security. Yet in a fact sheet dated that same month, the Commission expressed concerns that smaller European ports that lack the resources to participate in CSI would be discriminated against by shippers seeking to minimize security hassles.[38] The Commission believes, according to the document, "that security concerns would be addressed in a more effective manner by a pan-European measure as it would ensure homogeneous actions by EU administrations which are jointly in charge of managing the external trade of the EC throughout its single customs territory." It also noted that "the European Commission has initiated infringement procedures against those Member States that have entered into these bilateral agreements with the US, believing this within the scope of the Common Customs Policy."[39]

On November 18, 2003, the United States signed a reciprocal security agreement that effectively ended the EC's legal action against member states that choose to participate in the CSI—although officially, the infringement proceedings remain "on hold."[40] If approved by the European Council, the new trade security accord will represent an expansion of the 1997 EU-US Customs Cooperation Agreement. The key principle of the new agreement is reciprocity, meaning that whatever security requirements are applied to one party will also be applied to the other. A working group will be formed to hammer out the technical details of the expanded EU-U.S. cooperation.[41]

Although the United States and Europe seem to have resolved initial tensions over CSI, the merit of the EC's original objections—that the CSI may discriminate against smaller and nonparticipating ports—remains undetermined. For Europe, the solution to potential discrimination has been to expand the program. Commissioner Bonner has announced that, when fully implemented, CSI will represent "nearly 100 percent of all containerized cargo shipped from Europe to the United States."[42] For ports outside of Europe, however, particularly modest facilities in developing countries, the concern that the CSI will shift trade toward larger facilities still looms.

European governments in particular have raised concerns about potential port discrimination under CSI.

Expense. CSI has substantial costs, both direct and indirect. Shippers, freight forwarders, and shipping lines may have to upgrade their systems in order to meet requirements to provide timely information to Customs in electronic form. Those same parties must hire new security personnel and face potential delays at borders. Gamma and X-ray machines, advanced container locks, and bio-sensors all cost money, too.

The indirect costs of CSI could be much higher if the program forces companies to substantially alter longstanding business practices. After all, the point of international trade is to allow countries and companies to exploit their comparative advantages and produce more goods and services with fewer resources. Whenever new security measures reduce trade, they undermine the productivity gains that trade makes possible. Those gains are clearly visible at the firm level. Research by Accenture, Insead, and Stanford University found that companies with the most effective global supply chains achieved a compound annual growth rate in market capitalization that was 7–26 points greater than industry averages.[43]

So far, there is scant evidence that heightened border security measures have appreciably lessened trade.[44] It is likely, though, that any impact that CSI may eventually have on production and trade patterns will happen gradually. Yossi Sheffi, director of the Massachusetts Institute of Technology's Center for Transportation Studies, has speculated on how businesses might alter operations. In addition to increasing inventories, he suspects that companies will seek to insure themselves against border or port disruptions by shifting a portion of their supply contracts to local producers. Such changes, Sheffi predicts, will be neither large nor immediate. "It is unlikely that companies will forgo the benefits of low-cost, high-quality offshore manufacturing altogether," he writes. "[They] will only hedge their bets with local suppliers."[45]

The point of international trade is to allow countries and companies to exploit their comparative advantages.

There is at least some anecdotal evidence to support Sheffi's view that any impact of security on longstanding business practices will be gradual. Proctor & Gamble, for example, reports that new security procedures may spur changes in the way it conducts business. Specifically, the company's global cross-border organization group has recommended building up slightly higher inventories and forming new relationships with domestic suppliers.[46]

The cost of new security measures in terms of lost efficiency is unclear, but some assessments have been fairly pessimistic. According to Chip White, chair of the Transportation and Logistics School of Industrial and Systems Engineering at the Georgia Institute of Technology, new security measures are beginning to adversely impact supply-chain logistics. Looking specifically at CSI, White found that moving inspections from U.S. to foreign ports increases uncertainty. One reason is that when a container is delayed before it is loaded, it may miss its departure ship and then wait several days to sail. By contrast, shipments that have arrived in U.S. ports may be delayed by Customs, but the availability of regular truck and train service means that the shipment will generally be able to move once the container has been inspected. Although no formal surveys have been conducted, White says there is anecdotal evidence suggesting that lead times at some foreign ports have risen by 3–4 days, or 30–40 percent.[47]

In the public sector, governments in developing countries have expressed concerns about the cost of CSI. At a recent WTO meeting, for example, members of India's delegation argued that CSI "may penalize developing countries who may not be able to afford the installation of the required facilities at their ports, and thus be unable to join the U.S. initiative."[48] The United States has provided some limited funding and equipment to CSI ports. One CBP official recently reported that Personal Radiation Devices and Radio-Isotope Identifier Devices have been distributed to various CSI ports.[49] Much of the cost of upgrading security will be borne by foreign ports and governments, however, so issues of implementation are likely to continue to surface.

The global cargo container trade is still far from secure, but CSI is beginning to address some of the system's shortcomings. More U.S.-bound containers are being inspected sooner

and high-risk shipments are receiving additional scrutiny. At the very least, CSI has stirred a worldwide debate on how to make trade more secure. So far, disputes over the program have been relatively mild. This situation could change as CSI advances and the gap between processing times for compliant and noncompliant shippers and ports grows. Ports in developing countries and shippers forced to adopt new security technologies will likely complain loudest about the program. The integration of shippers' computer systems with Customs' AMS network, as well as the phasing out of paper manifests, will also continue to cause headaches.

More seriously, CSI has some apparent gaps. For example, bulk shipping—such as liquid natural gas, coal, iron ore, or grain—has received little attention under CSI. Many bulk cargos, such as ammonium nitrate fertilizer, can be volatile under the right conditions and could feasibly be used to turn a ship into a massive conventional bomb. Yet the International Maritime Organization rules that govern trade in bulk cargos were designed to prevent accidents, not intentional sabotage. In addition, any of the world's more than 23,000 registered bulk/general cargo vessels could be used to smuggle people or weapons into the United States. Bulk shipping presents risks nearly equal to those of container shipping, risks that deserve equal scrutiny.

CSI may require deepening as well as widening. The program relies on bill of lading information to target risky shipments for additional screening, yet currently no robust system exists for verifying the accuracy of such information, which shippers usually receive secondhand. Even when information is accurate, it is unlikely that Customs is currently receiving a complete risk profile of each shipment. For example, not all bills of lading contain information about prior handling or where a shipment was prior to the originating port.[50] The CBP's Automated Targeting System was designed to find narcotics, not weapons, and the General Accounting Office reports that the software is not fully consistent with current anti-terrorism modeling practices, meaning that it may not be doing the best job of screening for risky shipments.[51] And some critics have charged that Customs lacks a systematic program of random inspections adequate to test the accuracy of its targeting program.[52]

As CSI and similar programs evolve, policymakers should keep an open mind about the details of their rules. Some logistics experts have pointed out, for example, that the 24-hour rule might be less detrimental to efficiency if it were *extended.* The reasoning is that ports can better sort arriving containers if they have advance notice of which ones are likely to be scanned or inspected. 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.

The ultimate test of CSI, however, will come in the next phase of its implementation, when it seeks to change how technology is applied to shipping. CSI's greatest challenge will be moving container shipping toward something akin to the Total Asset Visibility and Authentication model used by the U.S. military. As it moves toward this goal, DHS should avoid attempting to mandate any particular technologies and instead focus on setting baselines for performance and promulgating open standards. It will be quite a challenge to gain widespread international adoption of interoperable technology without undermining incentives for innovation—and meeting that objective will likely necessitate extensive multilateral cooperation.

Customs-Trade Partnership against Terrorism

Launched in January 2002, the Customs-Trade Partnership against Terrorism was one of the first post-9/11 security initiatives. The goal of C-TPAT is to press the private sector into the terror-prevention business, from when a container is loaded until it reaches its destination. C-TPAT participants agree to meet minimum security standards in areas such as loading and unloading, cargo container seals, physical

The global cargo container trade is still far from secure, but CSI is beginning to address some of the system's shortcomings.

As CSI and similar programs evolve, policymakers should keep an open mind about the details of their rules.

security of buildings, access controls in cargo-handling and storage areas, employee screening and security training, manifest procedures, and conveyance security.[53]

One of C-TPAT's strengths is that it is a voluntary program that relies on incentives. In exchange for embracing measures to secure the business supply chain and submitting to government validation of its compliance with security stands, a business that participates in C-TPAT is offered expedited processing at U.S. ports of entry.

Because shorter border waits are valuable, C-TPAT has expanded rapidly. In its first year, more than 1,600 companies signed on; currently, the program has over 5,000 companies participating, representing more than 40 percent of the volume by value of imports in to the United States.[54] (However, only 130 of these companies had been validated as "C-TPAT certified" companies as of late 2003.[55]) Participants span the spectrum of trade, from manufacturers to air carriers to shipping lines to warehouses. "All major shippers, importers, and third-party logistics providers are working to get C-TPAT certified," reports Adrian Gonzalez of ARC Advisory Group. "Part of the reason why you see such high adoption in the C-TPAT program is because there was a level of collaboration between the government and the shipping community in establishing the program."[56]

Free and Secure Trade, or FAST, is the part of C-TPAT that is intended to speed commercial crossings across the U.S. borders with Canada and Mexico. The program is targeted to importers, road carriers, and truck drivers. In a nutshell, the program works as follows: When a C-TPAT-approved carrier is hauling qualifying goods from a C-TPAT-approved importer, and Customs receives advanced electronic transmission of information about the shipment, then the shipment can be pre-cleared for expedited border crossing through dedicated FAST lanes. All drivers using FAST lanes must possess a valid FAST-Commercial Driver Card, which requires background checks to assess whether a driver is a security risk.

Judging by the growing number of participants and by comments in trade publications, C-TPAT seems to have been relatively well received by the private sector. Indeed, some foreign shippers have been downright enthusiastic about the program. Captain Wei Jiafu, president of the major global shipping conglomerate China Ocean Shipping (Group) Co., for example, has championed C-TPAT to his colleagues: "The COSCO Group strongly encourages all companies that make up the global supply chain—especially its trading partners, terminals, and vendors—to become part of C-TPAT."[57] Similar praise has come from U.S. companies impressed with Custom's commitment to taking their concerns with the program into account.[58]

The next phase of C-TPAT (along with CSI) will reportedly involve attempts to develop a "smart and secure container" that is trackable and can detect and possibly report intrusions.[59] Smart container technology will be addressed in the final section of this paper.

Air Freight Security

The events of 9/11 proved that aircraft can be used for violence as well as for trade and travel. Hijacking inflicts direct damage, but airplanes can also be used to bring down buildings, hit military and industrial targets, or even speed WMDs into the heart of major U.S. cities. U.S and foreign carriers transport millions of packages each year, on both passenger and all-cargo planes. (Typically, about half of the hull of each passenger aircraft is filled with cargo.) In 2000 about 12.2 billion revenue ton miles (one ton of cargo transported one mile) of freight were shipped within the United States by air.[60] Many U.S. businesses have become reliant on sky borne commerce to move goods rapidly around the world, and the Department of Transportation projects that the amount of freight transported by air will increase rapidly in the years ahead.[61]

The Transportation Security Administration was created in November 2001 by the Aviation and Transportation Security Act as an arm of DOT.[62] ATSA transferred primary responsibility for securing air freight from the Federal Aviation Administration to TSA. It requires TSA to screen all cargo carried aboard commercial passenger aircraft and implement as soon as

possible a program to screen or otherwise ensure the security of cargo on all-cargo aircrafts. ATSA also mandated that all checked airline bags be screened by explosive detection systems by December 31, 2002, but no timetable was specified for screening cargo.[63]

Because of the expensive and highly visible nature of attacks on airlines, security in the cargo shipping industry tends to be more advanced than for other modes of transport. As a result of the 1988 Pan Am flight 103 bombing, Congress required the FAA to begin an accelerated schedule to find an effective explosive detection system to screen baggage and cargo. Today, freight forwarders and air carriers are required to have TSA-approved cargo-security programs, and only freight forwarders with approved programs are allowed to ship freight on passenger aircraft.

TSA inspectors have, however, identified vulnerabilities in security procedures of some air carriers and freight forwarders. One weakness is inadequate background checks for cargo handlers. There is also a potential for freight tampering. As with other modes of transport, the movement of cargo by air involves many parties. Manufacturers turn over cargo to shippers, about 80 percent of whom send the materials to freight forwarders that consolidate shipments and deliver them to air carriers.[64] At the departure airport, cargo is often first sent to a storage facility before being loaded onto an aircraft.[65] Shipments have the potential to be compromised at each of these points, especially when cargo is transported by land to the airport or handling facilities.

The Known Shipper program, which allows shippers that have established business histories with air carriers or freight forwarders to ship cargo on passenger planes, is TSA's primary approach for ensuring air cargo security. On an average day, TSA's Known Shipper database receives approximately 1,000 inquiries about particular shipments. About 60 percent of those are deemed to be from "unknown shippers." The database alerts carriers that those shipments must be rejected for transport on a passenger plane and diverted to an all-cargo aircraft or alternate form of transport.[66]

Coast Guard's "Maritime Domain Awareness"

The Coast Guard is in the process of developing a set of procedures and technologies collectively called Maritime Domain Awareness. The concept is for DHS to integrate information from intelligence agencies, commercial shippers, satellites, Customs, and other sources to create a complete picture of what vessels are in or near U.S. waters at any given time. Ships coming within 12 miles of the United States will be required to carry Automatic Identification Systems to track their locations. The Coast Guard will know not only the position of ships, but also who and what is onboard. Finally, Armed Coast Guard Sea Marshals will board and inspect ships that are 12 miles or more offshore to make sure they are safe to enter port.

National Targeting Center

In October 2001, U.S. Customs established the National Targeting Center to coordinate information from various agencies and sources and use that information to target attention on the riskiest cargo containers, ships, and personnel. NTC makes use of the Advance Targeting System—a software package that assembles and screens commercial, transportation, and passenger data to identify high-risk imported cargo and arriving international passengers. The NTC will be an integral part of CSI, C-TPAT, and other trade-security programs.

International Ship and Port Facility Security Code and the Safety of Life at Sea Convention

The 2001 attacks on the United States prompted the 158 member nations of the International Maritime Organization—a United Nations agency—to take coordinated multilateral action to improve shipping security. In February 2002 the IMO's maritime safety working group submitted a proposal intended to address four major areas: vessel tracking, port and ship security, cargo and container integrity, and verification of seafarer identity. The provisions concerning seafarer identity were subsequently stripped (it was decided that the International Labor Organization should deal with that issue) and the IMO approved a final package of

The next phase of C-TPAT will reportedly involve attempts to develop a "smart and secure container" that is trackable and can detect and possibly report intrusions.

The 2001 attacks on the United States prompted the 158 member nations of the International Maritime Organization to take coordinated multilateral action to improve shipping security.

reforms in December 2002. Much of the American Maritime Transportation Security Act of 2002 is devoted to enacting the security-related modifications of the Safety of Life at Sea (SOLAS) Convention and International Ship and Port Facility Security Code into U.S. law.

The ISPS Code is the set of IMO regulations designed to help detect and deter threats to commercial shipping. The 2002 revision of the code is divided into two parts. Part A consists of concrete security provisions, with little room for discretion, that are mandatory for all contracting governments. Part B lists more general voluntary measures intended to offer guidance for nations designing a maritime security plan. All ships and ports subject to the ISPS Code—meaning all ships weighing more than 500 tons and the ports that serve them—must implement the Part A mandatory requirements by July 1, 2004. These requirements include:

- A Ship Identification Number to be permanently marked on vessel hulls
- A Continuous Synopsis Record kept onboard showing vessel history
- The creation of a Ship or Port Facility Security Assessment Ship or Port Facility Security Plan
- Ship or Port Facility Security Certificate
- The hiring of a Ship or Port Facility Security Officer
- The hiring of a Company Security Officer
- Establishment of a continuous ship-to-port security communication link
- Regular training and drills
- Installation of a ship security alert system

It should be noted that Part B—the 60-page "voluntary" component of the ISPS Code revisions—is considered mandatory by the United States. This means that both U.S. shippers and ports and foreign shippers and ports that do business with the United States will be expected to comply with both parts of the revised ISPS code. The Coast Guard has estimated that compliance with all ISPS regulations by the U.S.-flagged fleet will cost about $1.4 billion between 2003 and 2012, while U.S. ports and related facilities would have to spend some $5.4 billion over the same period.[67] Most of these funds will go toward hiring new security personnel, purchasing and installing equipment, and complying with reporting requirements. Some analysts, however, have speculated that the real costs will be far higher.[68]

U.S. Bioterrorism Preparedness and Response Act

In response to the anthrax attacks on U.S. citizens following 9/11, Congress passed the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 (the "Bioterrorism Act").[69] The rules promulgated under this legislation were scheduled to go into effect on December 12, 2003. However, the World Shipping Council reports that the U.S. Food and Drug Administration—charged with enacting U.S. bioterrorism countermeasures—has implemented a grace period to allow exporters and shipping lines time to adjust to the new rules. When fully implemented, the WSC estimates that the Bioterrorism Act will apply to 12 percent of cargoes shipped to the United States, currently worth some $50 billion per year.[70]

In some respects, the Bioterrorism Act appears to be the most burdensome trade-security legislation passed by Congress to date. Regulations promulgated under the Act require every facility in the world that produces or stores food bound for the United States to register with the FDA and have a U.S. agent. They mandate the advance submission of detailed information—including the names of all growers, which are often not available for commodities like coffee or coca beans—about each shipment prior to its arrival. Shipments that fail to comply with these rules will be detained for up to 30 days, meaning that spoilage could become a major issue for perishable products.[71]

Food importers and shippers have expressed particular apprehension over how and when the FDA will detain shipments. There is uncertainty about what will trigger enforcement. Companies have noted that mistaken delays could be very costly, both in terms of ruined foodstuffs and idled equipment such as trucks. And there are questions about how much addi-

tional security will actually be achieved. Commenting on the Bioterrorism Act's registration requirements, one business noted:

> Responsible importers are already doing such things anyway, even from the point where produce is growing in the field in foreign countries . . . and the USDA are also doing their part. . . . To request legitimate businesses put up more paperwork with the FDA in this regard is only a redundant paper chase and should be discouraged.[72]

Given these concerns, Congress should be vigilant in overseeing the FDA's activities with respect to the Bioterrorism Act. In doing so, Congress should ask the following: Would the FDA even be able to detect at the border a biological attack via food imports if one were to occur? Are the FDA, CBP, and the Department of Agriculture performing redundant roles? Does the Act discourage agricultural exports bound for Mexico or Canada from landing at U.S. ports? The answers to these and other questions should be resolved if this program is to move forward.

Trade Security and Technology: Smart Containers and Asset Visibility

The future of trade security will rely heavily on technology. There will never be enough human inspectors to look into every cargo container, truck, and rail car. Cargo cannot be guarded 24 hours a day. Technology promises to bridge the manpower gap by enabling the continual monitoring and tracking of freight.

The use of electronics is already prevalent in commercial shipping. Cameras observe storage and loading areas at factories, ports, and warehouses. Digital identification cards restrict access to sensitive areas and store digital information about employees, including photographs, and increasingly, biometric data. Information about a cargo container's contents is electronically transmitted to Customs officials before the container is even loaded onto a ship.

Ironically, the single most visible element of the trading system—the cargo container—remains stubbornly low-tech and notoriously insecure. Indeed, instructions on how to break into a shipping container in under two minutes are readily available on the Internet.[73] Most container seals currently in use are designed to detect intrusion, not stop it. Yet even in that limited role, many container seals are easily defeated.

Smart Containers

Efforts are already underway to elevate the image of the lowly "dumb" cargo container. Congress is encouraging the administration to "test technologies that enhance port of entry operations, including those related to inspections, communications, port tracking, identification of persons and cargo, sensory devices, personal detection, decision support, and the detection and identification of weapons of mass destruction."[74] DHS is currently running Operation Safe Commerce, a collection of 18 TSA-funded public-private projects that focus on container supply chain security shortcomings from point of origin to point of destination. OSC projects test new procedures and off-the-shelf technology solutions in an operational environment. They cover container tracking and tracing, nonintrusive detection strategies, and improved container seals. Programs like C-TPAT and CSI are integrated into many of the projects. Tests are ongoing at the nation's top three load centers: New York/New Jersey, Seattle/Tacoma, and Los Angeles/Long Beach. TSA expects to use OSC results to develop container supply chain best practices and standards for use by commercial maritime shippers.

A large number of companies are vying to provide trade-security solutions. They offer a bewildering array of products, from tamper-evident chemical seals to strong mechanical locking mechanisms to advanced satellite-tracking technologies. The most interest and attention, however, has revolved around efforts to create a "smart container" that greatly improves the ability of shippers, cargo owners, and Customs

In some respects, the Bioterrorism Act appears to be the most burdensome trade-security legislation passed by Congress to date.

agents to know when a container has been opened or diverted. Smart containers offer the promise of strong security from the time a container is loaded until the time it reaches its final destination.

The most basic smart containers would probably incorporate passive radio frequency identification (RFID) tags—technology similar to that used to track cars through toll lanes—that would be read by either handheld or stationary scanners. The RFID tags would store information about the container's contents and its travels. More advanced RFID solutions would include a hybrid electronic/mechanical seal that both bars and detects unauthorized container entry. If a container is opened during transit, the seal would record information about when (and possibly where) the intrusion occurred.

Passive RFID technology has several advantages, including relatively low cost and proven operational capability. Tags are activated by scanners and thus do not require a power source. Passive seals have drawbacks, too. They provide for only limited tracking of containers in transit. Stakeholders can see when a particular container arrives at a port, warehouse, or other scanning station, but real-time tracking is not available with passive RFID and containers do not alert anyone at the moment they are compromised.

More sophisticated smart containers could include active electronic seals. These devices would detect when someone breaks into a container and would have the ability to communicate that information to a shipper, customs, or cargo owner via satellite, radio, or cellular—or conceivably, even local Wi-Fi computer networks installed on ships and at ports. In the most advanced versions, cargo containers could be outfitted with Global Positioning System devices for precise location tracking and sensors to detect and alert authorities immediately to the presence of chemical, biological, or nuclear elements.

A *Wall Street Journal* article recently described how active-seal smart containers might work:

> [A smart container] could say, 'Hey, someone has taken me to a place off my route, and I was there for two days. Is that OK?' says Blair LaCorte, an executive vice president of Savi Technology Inc. The Sunnyvale, Calif., company has already set up a system using radio-frequency identification technology to track about 25,000 containers a day for the Department of Defense. Such systems include a radio transmitter and receiver on the container, which is linked to a central data system.[75]

Not surprisingly, active-seal technology is more expensive than passive-seal technology—up to 10 times more expensive, according to the U.S. Treasury's Advisory Committee on Commercial Operations of the U.S. Customs Service.[76] Active seals also require a power source and are unproven on a mass scale. Fortunately, DHS need not mandate a single solution. As long as a seal can communicate with CBP scanners, it does not necessarily matter whether a container uses active or passive technology. Nor is it critical that all containers have exactly the same package of features. By setting standards and avoiding overly detailed mandates, DHS can preserve a dynamic, competitive marketplace for smart-container technology that continues to yield advances over time.

Instructions on how to break into a shipping container in under two minutes are readily available on the Internet.

Security and Asset Visibility: A Win-Win?

"Asset visibility" refers to the ability of buyers and sellers to track shipments en route. In many cases, strong asset visibility allows a company to manage its supply chain more effectively, squeezing inventories and improving operational efficiency. In theory, many of the security technologies on the horizon, such as smart containers, would improve asset visibility, and thus, productivity. The hope is that these technologies will boost both security and profitability.

Unfortunately, such a happy outcome is unlikely to be obtained in all cases. If improved security paid for itself, it might be expected that more companies would already be pursuing it voluntarily. And even when better asset visibility can make supply chains more efficient, companies must have the incentive (and

ability) to solve or work around shipping delays once they are detected. In general, companies that operate very fast or slow supply chains are likely to see limited (or no) gains from improved asset visibility, whereas companies in the middle are most likely to benefit.

The reason for this distinction is that a company with either a high- or low-velocity product cycle is already locked into supply decisions. Consider the situation faced by an American computer manufacturer that runs a just-in-time production facility that relies on hard drives imported from Asia. Because the company's business plan depends on the timely delivery of every component that goes into a computer, and because hard drives have a relatively high value-to-weight ratio, the company will almost certainly ship the drives by air. In addition, since timing is critical for companies that pay a premium for air transit, carriers strive to provide current information about a shipment's status. In other words, asset visibility in this case is already very high and new security technologies will not necessarily enhance productivity.

At the other end of the spectrum would be a big box retailer like Home Depot that purchases thousands of varieties of retail goods in large quantities. Because no single shipment is critical for overall operations, the company requires only a rough idea of when a particular product will arrive. Heightened asset visibility might be nice, but knowing that a shipment of hammers has been delayed in Hong Kong, for example, will not prompt the company to pay a premium to expedite supply. The value-to-weight ratio of the retailer's imports is generally too low to consider alternative modes of transport (i.e., air) to overcome small delays.

Some companies will undoubtedly be able to use better asset visibility to streamline their operations. The emerging consensus, however, seems to be that "win-win" scenarios where security improvements pay for themselves through greater efficiency will not be the rule. As one expert has speculated, CSI and other such programs are "at best zero in terms of productivity improvement and at worst significantly negative."[77] This does not mean that improving cargo tracking is not a worthwhile security goal. It does, however, suggest that the transition will be more costly than many have hoped.

Protection versus Protectionism

The Bush administration has so far taken a relatively conservative risk-reduction approach to trade security: Programs such as CSI and C-TPAT seek to remove major vulnerabilities from the system while recognizing the need for trade to keep flowing. DHS has been willing to accept some tradeoff between security and efficiency, but it does not assert that its programs are—or could be—foolproof.

That is not enough for some members of Congress. H.R. 1010, for example, sponsored by Rep. Jerrold Nadler (D-NY), would require all cargo containers bound for the United States to be physically inspected, have their contents verified, and be sealed by personnel of the Department of Homeland Security at a port or airport outside the United States. The legislation would also require the Coast Guard to board and inspect every cargo ship bound for the United States at least 200 miles offshore to make sure that containers had not been compromised en route.[78]

H.R. 1010 is a radical proposal, to say the least, and one that would have severe negative impacts on trade. Neither CBP nor the Coast Guard has anything near the resources or manpower to inspect every container before sailing and then reinspect it as ships approach the coast. Even if the resources were available, it is highly doubtful that foreign countries would agree to host the large Customs contingents necessary to carry out the bill's mandate.

When assessing the merit of such extreme legislation, it is instructive to note the voting record of its sponsors. In the case of H.R. 1010, Rep. Jerrold Nadler voted against every major piece of pro-trade legislation in the 107th Congress—a record that suggests a poor understanding of the importance of open global markets.[79]

Smart containers offer the promise of strong security from the time a container is loaded until the time it reaches its final destination.

If improved security paid for itself, it might be expected that more companies would already be pursuing it voluntarily.

Other legislation would set unreasonable security standards of questionable value. S. 1147, the High-Tech Port Security Act of 2003 sponsored by Sen. Barbara Boxer (D-CA), mandates that all cargo containers entering the United States after a 15-month phase-in period be certified as "blast resistant."[80] The legislation also directs that all U.S.-bound containers be screened for radioactive materials within the same time frame. Although blast-resistant containers might be useful for air freight, where an explosive device would be small, a maritime container's large size would allow for powerful bombs that could not be contained. And they would have no effect on nuclear devices, of course. The benefits for containerized shipping would thus be negligible and carry the extreme cost of replacing millions of containers. (Blast-resistant air cargo containers cost about 15 times more than standard containers; the difference would likely be even larger for the massive ship borne containers.) In sum, the merits of this legislation are questionable at best and deserve special scrutiny given Boxer's past lack of commitment to keeping international trade flowing. Indeed, the junior senator from California has one of the worst trade policy records in the Senate, voting to remove trade barriers just 13 percent of the time during the 107th Congress.[81]

Some legislation attempts to address real problems in questionable ways. The Port Security Improvement Act of 2003—H.R. 2193—was introduced by Reps. Doug Ose, (R-CA) and John Tierney (D-MA).[82] It would allocate 30 percent of all duties collected by Customs to the Department of Homeland Security. These funds would go to each port based on the amount of duties it collects. The federal government presently disburses security funds to ports on a competitive grant basis. Ose has noted that this has led to some seeming inequities. The Port of Los Angeles, for example, collected 32 percent of all U.S. duties in 2002, yet received only a small fraction of that money back for security improvements.[83]

H.R. 2193 raises the important issue of how port security should be funded. Unfortunately, by tying port funding to monies collected, the bill sets up incentives for security agencies to oppose lower tariffs. The proposal is especially questionable with the United States currently engaged in a range of bilateral, regional, and global negotiations intended to tear down tariff walls.

Finally, some legislation is not necessarily protectionist but has little connection to security. The first two stated goals of S. 1400, for example, sponsored by Sen. Olympia Snowe (R-ME), are "securing national security" and "advancing economic development." Yet the heart of the legislation is the establishment of an "Integrated Ocean and Coastal Observing System" charged with tasks such as "understanding, assessing, and responding to human-induced and natural processes of global change"; "supporting efforts to protect, maintain, and restore the health of and manage coastal and marine ecosystems and living resources"; "enhancing public health"; and "monitoring and evaluating the effectiveness of ocean and coastal environmental policies."[84] These may or may not be worthy activities, but they have little to do with homeland security. When falsely justified, spending on such projects robs taxpayers and diverts scarce funds from genuine security projects.

Of course, not all legislation on the horizon is ill advised. S. 165, The Air Cargo Security Act, was introduced by Sens. Kay Bailey Hutchison (R-TX) and Dianne Feinstein (D-CA), and passed by unanimous consent in the Senate on May 8, 2003. It is currently awaiting action by the House of Representatives. The bill is essentially identical to a bill passed the previous year that was sponsored by Sens. John McCain (R-AZ) and Ernest "Fritz" Hollings (D-SC).

S. 165 would require TSA to regularly inspect air-shipping facilities, expand the Federal Flight Deck Officer Program by allowing pilots of air cargo aircraft to be armed, establish an industry-wide database of cargo shippers, and create a security-training program for air cargo handlers. (The Congressional Budget Office projected that the costs of implementing these measures between 2004–2008 would total $417 million.) S. 165 would also allow eligible

cargo pilots, regardless of state laws, to carry firearms within and across state borders. The arming of pilots has been supported by pilot's unions and is a good example of providing low-cost incentives for the private sector to play a more active and vigilant role in security provision. On the regulatory front, S. 165 would impose private-sector mandates as defined in the Unfunded Mandates Reform Act on carriers that transport cargo and facilities that provide flight training to foreign candidates.[85]

Finally, although the legislative threat of protectionism masquerading as security lies largely in the future, DHS is already spending scarce resources on projects of little value. In 2003, for example, Customs seized more than $160 million in apparel shipments from China that violated quota restrictions.[86] Despite the fact that the United States will be scrapping its quotas in less than a year, Rep. Sue Myrick (R-NC) reports working with Customs to fund the development of a "textile tracer" that would determine the origin of U.S. textile imports.[87] Customs is struggling to search shipping containers for WMD, yet Myrick boasts that she has "also secured $9.5 million in funding to hire additional custom agents to guard our borders against these illegal textile goods coming in from other countries."[88] Considering what is at stake, there are better ways that those millions could be spent than "protecting" Americans from low-cost clothing.

Conclusion

The security of global trade is a never-ending project, one in which the government has a legitimate and leading role to play. The country must continue to be alert for ways to enhance security without closing borders. This will require an ongoing assessment of the costs and benefits of current and future trade-security initiatives. It will mean maintaining an openness to new technologies and the right incentives to develop them. It will rely on open lines of communication between intelligence agencies, homeland security agencies, ports, businesses, and state, local, and foreign governments.

Above all, an effective risk-reduction strategy will require a recognition that although the federal government can coordinate America's efforts, it cannot and should not be the sole provider of security. Private companies will, of necessity, be on the front lines of this conflict. Where regulations are necessary, companies should specify goals, set standards, and gauge progress rather than micromanage behavior. Companies should be encouraged not only to follow the letter of government directives, but to become responsible stakeholders in the terrorism-prevention business. Vigilance must become a mindset, not just a checkbox on a list of rules.

In this endeavor, stasis will be the enemy of safety. Terrorists will study whatever measures are adopted. They will probe for weaknesses and eventually find some. Successful attacks are probably inevitable. Yet a tough and adaptable trade-security system can give policymakers the confidence to keep the engine of trade running when something does go wrong. And with each incident, policymakers, agencies, and companies will have the opportunity to learn from their mistakes and make future attacks less likely.

Economic openness is a progressive force in global affairs. Trade brings nations together in peaceful cooperation, offers hope to the world's poorest people, and spreads new ideas and ways of doing things. Trade promotes democracy, private property, and the rule of law. Our enemies know this. They targeted the World Trade Center because they recognized—and continue to believe—that trade is a threat to the tyranny they represent.

Notes

1. For more on U.S. sectoral protectionism, see Daniel Ikenson, "Threadbare Excuse: The Textile Industry's Campaign to Preserve Import Restraints," Cato Trade Policy Analysis no. 25, October 15, 2003; and Mark Groombridge, "America's Bittersweet Sugar Policy," Cato Trade Briefing Paper no. 13, December 4, 2001. Both are available at http://www.freetrade.org.

2. The 21,000 cargo container figure was cited by Sen. Susan Collins, "Cargo Containers: The Next Terrorist Target?," opening remarks before the

The Bush administration has so far taken a relatively conservative risk-reduction approach to trade security.

Senate Committee on Governmental Affairs, March 20, 2003, http://www.senate.gov/~gov_affairs/032003collins.htm.

3. John Mintz, "15 Freighters Believed to Be Linked to al-Qaeda; U.S. Fears Terrorists at Sea," *Washington Post*, December 31, 2002.

4. "Bin Laden Still Alive: Al-Qaida," *Tribune* (India), July 11, 2002, http://www.tribuneindia.com/2002/20020711/world.htm.

5. Maarten van de Voort and Kevin A. O'Brien, "Seacurity: Improving the Security of the Global Sea-Container Shipping System," RAND Europe Report no. MR-1695-JRC, 2003, p. 3, http://www.rand.org/publications/MR/MR1695/MR1695.pdf.

6. Stefano Ambrogi, "Experts: Al Qaeda Maritime Threat Growing," *Reuters*, February 18, 2004.

7. Total seafarers in 2000 according to the *BIMCO/ISF Manpower Update Report*, April 2000, http://www.marisec.org/resources/2000Manpowerupdate.htm.

8. Ann Wise, Yael Lavie, and Brian Hartman, "Italian Police Probe Man Found in Box," *ABCNews.com*, October 27, 2001, http://abcnews.go.com/sections/us/DailyNews/wtc_investigation011027.html.

9. Mark Gerencser, Jim Weinberg, and Don Vincent, "Port Security War Game: Implications for U.S. Supply Chains," Booz Allen Hamilton, February 2003, http://www.bah.de/content/downloads/port_security. pdf.

10. Abt Associates, "The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability," executive summary, April 30, 2003, p. 7, http://www.abtassoc.com/reports/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf.

11. Figures cited in Robert C. Bonner, testimony before the U.S. Senate Committee on Commerce, Science and Transportation, September 9, 2003, http://usinfo.state.gov/topical/pol/terror/texts/03091523.htm.

12. Robert C. Bonner, Customs Commissioner, Hearing on Security at U.S. Seaports, U.S. Senate Committee on Commerce, Science, and Transportation, Charleston, South Carolina, February 19, 2002, http://commerce.senate.gov/hearings/021902bonner.pdf.

13. Statistic cited in "Why Trade Is Good for U.S. Manufacturing," multiagency U.S. government fact sheet, http://www.tpa.gov/manufacturing.htm.

14. Figure cited in General Accounting Office, "Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process," GAO-03-782, July 2003, p. 4.

15. Quoted at http://www.gmu.edu/departments/economics/bcaplan/pubcho1.html.

16. This idea has been recently put into practice in H.R. 2122, the Project Bioshield Act.

17. David Haarmeyer and Peter Yorke, "Port Privatization: An International Perspective," Reason Foundation Policy Study no. 156, April 1993, http://www.rppi.org/privatization/ps156. PDF.

18. Philippe Crist, "Security in Maritime Transport: Risk Factors and Economic Impact," Organisation for Economic Co-operation and Development, July 2003, p. 25, http://www.oecdwash.org/DATA/DOCS/security_in_maritime_transport.pdf.

19. Ibid.

20. See report of the U.S. Treasury Advisory Committee on Commercial Operations of the United States Customs Service, Subcommittee on U.S. Border Security Technical Advisory Group, and Customs Trade Partnership against Terrorism, vol. 1, p. 5, June 14, 2002.

21. Ibid., p. 2.

22. Remarks at the port of Charleston, South Carolina, February 5, 2004.

23. U.S. Customs and Border Protection, "Frequently Asked Questions about CSI," http://www.customs.ustreas.gov/xp/cgov/enforcement/international_activities/csi/q_and_a.xml.

24. Crist, p. 10.

25. Ibid.

26. Ibid., p. 14.

27. http://www.cbp.gov/xp/cgov/enforcement/international_activities/csi/csi_in_brief.xml.

28. "U.S. Customs Service's Container Security Initiative," State Department Fact Sheet, February 22, 2002, http://usinfo.state.gov/topical/pol/terror/02022505.htm.

29. Figure taken from "U.S. Customs and Border Protection: Response to Terrorism," Powerpoint presentation, http://www.customs.ustreas.gov/ImageCache/cgov/content/import/cargo_5fcontrol/csi/minimum_5fstandards_2epps/v1/mini

mum_5fstandards.pps.

30. Ports categorized as "coming soon" by the U.S. Department of Homeland Security: Algeciras (Spain); Colombo (Sri Lanka); Laem Chebang (Thailand); Port Kelang and Tanjong Pelepas (Malaysia); Tokyo, Nagoya, Kobe, and Osaka (Japan); Shenzhen and Shanghai (China); and Durban (South Africa). See http://www.cbp.gov/ImageCache/cgov/content/import/cargo_5fcontrol/csi/ports_5fcsi_5flandscape_2epps/v1/ports_5fcsi_5flandscape.pps.

31. Customs and Border Protection, "Minimum Standards for CSI Expansion," undated slide presentation, http://www.cbp.gov/ImageCache/cgov/content/import/cargo_5fcontrol/csi/standard_5fcurrent_5fgeneric_2epps/v1/standard_5fcurrent_5fgeneric.pps.

32. A bill of lading is a document issued by a carrier (railroad, ship, or trucking company) that serves as a receipt for the goods to be delivered to a consignee. The bill describes the conditions under which the goods are accepted by the carrier and details the nature and quantity of the goods, name of vessel, identifying marks and numbers, destination, and so on.

33. Customs and Border Protection, "Customs Issues 'No-Load' Directives on the 24-Hour Rule," press release, February 13, 2003, http://www.cbp.gov/xp/cgov/newsroom/press_releases/022003/02132003.xml.

34. "General Update on Initiatives to Increase Maritime Security in the USA," *P&O Nedlloyd News*, September 30, 2003, http://www.ponl.com/topic/home_page/language_en/newsroom/news/latest_news?resourceitem_no=10376&usetemplate=latest_news_item.

35. Robert C. Bonner, "Securing America's Borders While Safeguarding Commerce," Heritage Lecture no. 796, September 9, 2003, p. 5, http://www.heritage.org/Research/HomelandDefense/HL796.cfm.

36. Irvin Lim Fang Jau, "Not Yet All Aboard . . . but Already All at Sea over the Container Security Initiative," *Journal of Homeland Security Studies*, November 2002, http://www.homelandsecurity.org/journal/Articles/Jau.html.

37. Nigel Brew, "Ripples from 9/11: The US Container Security Initiative and Its Implications for Australia," Department of the Parliamentary Library, Current Issues Brief no. 27 2002-03, May 13, 2003.

38. "Container Security," European Union Factsheet, June 25, 2003, http://europa.eu.int/comm/external_relations/us/sum06_03/cs.pdf.

39. Ibid.

40. "EU/US: Accord Initialed to Bolster Container Security," *European Report* 2821, November 19, 2003.

41. "Brussels Signs Box Security Deal with US," *Lloyd's List*, November 19, 2003.

42. Statement of Robert C. Bonner, December 20, 2002, http://www.useu.be/Categories/Justice%20and%20Home%20Affairs/Dec2002BonnerECCSIStatement.html.

43. Results reported in Sarah Murray, "World Risk: Alert—Importers Pay the Price of Heavy Security," *Economist Intelligence Unit RiskWire*, January 13, 2004.

44. Rear Admiral Larry L. Hereth makes this point in testimony before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, January 27, 2004, http://judiciary.senate.gov/print_testimony.cfm?id=1016&wit_id=2920.

45. Yossi Sheffi, "Supply Chain Management under the Threat of International Terrorism," *International Journal of Logistics Management* 12, no. 2 (2001): 3.

46. David Hannon, "Securing the Supply Chain: What You Need to Know Today," *Purchasing*, January 15, 2004, p. 15.

47. Estimate given in a January 30, 2004, conversation with the author.

48. John Zarocstas, "US Security Clamp Is a Barrier to Trade WTO Delegates Warn," *Lloyd's List*, January 21, 2004, p. 16.

49. Robert M. Jacksta, executive director for Border Security and Facilitation, Office of Field Operations, Customs and Border Protection, testimony before the Senate Judiciary Subcommittee on Terrorism, Technology and Homeland Security, January 27, 2004, http://judiciary.senate.gov/print_testimony.cfm?id=1016&wit_id=2921.

50. This gap was pointed out by World Shipping Council president Christopher Koch in remarks before the Panama Canal Authority's Conference on Maritime Security, December 1, 2003, p. 12.

51. Richard M. Stana, testimony before the House of Representatives Committee on Energy and

Commerce, Subcommittee on Oversight and Investigations, GAO-04-325T, December 16, 2003, p. 10.

52. Sen. Joseph Lieberman (D-CT) made this charge. "Sen. Lieberman Issues Top 10 To-Do List for Homeland Security in 2004," *States News Service*, January 23, 2004.

53. See http://www.cbp.gov/ImageCache/cgov/content/import/commericial_5fenforcement/ctpat/validation_5fprocess/validation_5fprocess_5fguidelines_2epdf/v1/validation_5fprocess_5fguidelines.pdf.

54. Robert C. Bonner, testimony before the National Commission on Terrorist Attacks upon the United States, January 26, 2004.

55. Robert C. Bonner, testimony before the House Select Committee on Homeland Security Subcommittee on Infrastructure and Border Security, October 16, 2003.

56. Hannon, p. 15.

57. Letter from Captain Wei Jiafu, president of the China Ocean Group Shipping Company, May 30, 2003, http://www.cosco-usa.com/omd/security/captweiltr.pdf.

58. R. G. Edmonson, "Carriers Praise Homeland Security," *Journal of Commerce Online*, March 2, 2004, http://www.joc.com.

59. Koch, p. 14.

60. General Accounting Office, "Aviation Security: Vulnerability and Potential Improvements for the Air Cargo System," GAO-03-344, December 2002, p. 1.

61. General Accounting Office, "Aviation Security: Vulnerability and Potential Improvements for the Air Cargo System," GAO-03-344, December 2002, p. 5.

62. P.L. 107-71.

63. Air Cargo Security Improvement Act, Report of the Committee on Commerce, Science, and Transportation on S. 165, April 24, 2003, p. 2.

64. General Accounting Office, "Aviation Security: Vulnerability and Potential Improvements for the Air Cargo System," GAO-03-344, December 2002, p. 4.

65. Ibid., p. 3.

66. E-mail exchange with Deirdre O'Sullivan, public affairs specialist with the Transportation Security Administration, February 27, 2004. Thanks to Cato Institute's Tudor Rus for research assistance on this issue.

67. Beth Jinks, "US Coast Guard Demands Exceed IMO Security Rules," *Shipping Times* (Singapore), December 16, 2003, http://business-times.asia1.com.sg/story/0,4567,102756,00.html.

68. Such as Robert Force of the Maritime Law Center at Tulane, quoted in ibid.

69. P.L. 107–188. See http://www.fda.gov/oc/bioterrorism/PL107-188.html.

70. Rainbow Nelson, "Bioterrorism," *Lloyd's List*, December 3, 2003, p. 3.

71. See http://www.fda.gov/oc/bioterrorism/bioact.html.

72. Calum Turvey, Den Onyango, and Brian Schilling, "Impact of the 2002 Bioterrorism Act on the New Jersey Food Industry," Rutgers University Food Policy Institute Working Paper no. WP-0603-101, October 15, 2003, p. 9.

73. See http://www.sealock.com/problem/problem.htm.

74. S. 539/H.R. 1036, 108th Congress.

75. Daniel Machalaba and Andy Pasztor, "Thinking inside the Box: Shipping Containers Get 'Smart,'" *Wall Street Journal*, January 15, 2004.

76. Report of the U.S. Treasury Advisory Committee on Commercial Operations of the United States Customs Service, Technology Subcommittee, vol. 7, p. 6, June 14, 2002.

77. Quoted in Hannon, p. 15.

78. See H.R. 1010, 107th Congress, http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.1010.

79. Nadler voted "yes" only on Cuba travel, Vietnam NTR, and access to foreign doctors. See Daniel T. Griswold, "Free Trade, Free Markets: Rating the 107th Congress," Trade Policy Analysis no. 22, January 30, 2003, http://www.freetrade.org/pubs/pas/tpa-022.pdf.

80. S. 1147, 107th Congress.

81. Griswold, p. 35.

82. H.R. 2193, 107th Congress.

83. Doug Ose, "Financing Port Infrastructure:

Who Should Pay?" testimony before the House Transportation and Infrastructure Water Resources and Environment Subcommittee, November 20, 2003, http://www.house.gov/transportation/water/11-20-03/ose.pdf.

84. S. 1400, 108th Congress.

85. See "Air Cargo Security Improvement Act," report of the Committee on Commerce, Science, and Transportation on S. 165, April 24, 2003.

86. "Second Report to the Congressional Textile Caucus on the Administration's Efforts on Textile Issues," executive summary, U.S. Department of Commerce, October 2003.

87. Sue Myrick, "Trade Action a Good First Step," November 21, 2003, http://www.house.gov/apps/list/speech/nc09_myrick/ed112103_safeguards.html.

88. Ibid.

Trade Policy Analysis Papers from the Cato Institute

"Trading Tyranny for Freedom: How Open Markets Till the Soil for Democracy" by Daniel T. Griswold (no. 26; January 6, 2004)

"Threadbare Excuses: The Textile Industry's Campaign to Preserve Import Restraints" by Dan Ikenson (no. 25; October 15, 2003)

"The Trade Front: Combating Terrorism with Open Markets" by Brink Lindsey (no. 24; August 5, 2003)

"Whither the WTO? A Progress Report on the Doha Round" by Razeen Sally (no. 23; March 3, 2003)

"Free Trade, Free Markets: Rating the 107th Congress" by Daniel Griswold (no. 22; January 30, 2003)

"Reforming the Antidumping Agreement: A Road Map for WTO Negotiations" by Brink Lindsey and Dan Ikenson (no. 21; December 11, 2002)

"Antidumping 101: The Devilish Details of 'Unfair Trade' Law" by Brink Lindsey and Dan Ikenson (no. 20; November 26, 2002)

"Willing Workers: Fixing the Problem of Illegal Mexican Migration to the United States" by Daniel Griswold (no. 19; October 15, 2002)

"The Looming Trade War over Plant Biotechnology" by Ronald Bailey (no. 18; August 1, 2002)

"Safety Valve or Flash Point? The Worsening Conflict between U.S. Trade Laws and WTO Rules" by Lewis Leibowitz (no. 17; November 6, 2001)

"Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive" by Aaron Lukas (October 30, 2001)

"Trade, Labor, and the Environment: How Blue and Green Sanctions Threaten Higher Standards" by Daniel Griswold (no. 15; August 2, 2001)

"Coming Home to Roost: Proliferating Antidumping Laws and the Growing Threat to U.S. Exports" by Brink Lindsey and Daniel Ikenson (no. 14; July 30, 2001)

"Free Trade, Free Markets: Rating the 106th Congress" by Daniel T. Griswold (no. 13; March 26, 2001)

"America's Record Trade Deficit: A Symbol of Economic Strength" by Daniel T. Griswold (no. 12; February 9, 2001)

"Nailing the Homeowner: The Economic Impact of Trade Protection of the Softwood Lumber Industry" by Brink Linsey, Mark A. Groombridge, and Prakash Loungani (no. 11; July 6, 2000)

"China's Long March to a Market Economy: The Case for Permanent Normal Trade Relations with the People's Republic of China" by Mark A. Groombridge (no. 10; April 24, 2000)

"Tax Bytes: A Primer on the Taxation of Electronic Commerce" by Aaron Lukas (no. 9; December 17, 1999)

"Seattle and Beyond: A WTO Agenda for the New Millennium" by Brink Lindsey, Daniel T. Griswold, Mark A. Groombridge, and Aaron Lukas (no. 8; November 4, 1999)

"The U.S. Antidumping Law: Rhetoric versus Reality" by Brink Lindsey (no. 7; August 16, 1999)

"Free Trade, Free Markets: Rating the 105th Congress" by Daniel T. Griswold (no. 6; February 3, 1999)

"Opening U.S. Skies to Global Airline Competition" by Kenneth J. Button (no. 5; November 24, 1998)

Trade Briefing Papers from the Cato Institute

"Job Losses and Trade: A Reality Check" by Brink Lindsey (no. 19; March 17, 2004)

"Free-Trade Agreements: Steppingstones to a More Open World" by Daniel T. Griswold (no. 18; July 10, 2003)

"Ending the 'Chicken War': The Case for Abolishing the 25 Percent Truck Tariff" by Dan Ikenson (no. 17; June 18, 2003)

"Grounds for Complaint? Understanding the 'Coffee Crisis'" by Brink Lindsey (no. 16; May 6, 2003)

"Rethinking the Export-Import Bank" by Aaron Lukas and Ian Vásquez (no. 15; March 12, 2002)

"Steel Trap: How Subsidies and Protectionism Weaken the U.S. Industry" by Dan Ikenson (no. 14; March 1, 2002)

"America's Bittersweet Sugar Policy" by Mark A. Groombridge (no. 13; December 4, 2001)

"Missing the Target: The Failure of the Helms-Burton Act" by Mark A. Groombridge (no. 12; June 5, 2001)

"The Case for Open Capital Markets" by Robert Krol (no. 11; March 15, 2001)

"WTO Report Card III: Globalization and Developing Countries" by Aaron Lukas (no. 10; June 20, 2000)

"WTO Report Card II: An Exercise or Surrender of U.S. Sovereignty?" by William H. Lash III and Daniel T. Griswold (no. 9; May 4, 2000)

"WTO Report Card: America's Economic Stake in Open Trade" by Daniel T. Griswold (no. 8; April 3, 2000)

"The H-1B Straitjacket: Why Congress Should Repeal the Cap on Foreign-Born Highly Skilled Workers" by Suzette Brooks Masters and Ted Ruthizer (no. 7; March 3, 2000)

"Trade, Jobs, and Manufacturing: Why (Almost All) U.S. Workers Should Welcome Imports" by Daniel T. Griswold (no. 6; September 30, 1999)

"Trade and the Transformation of China: The Case for Normal Trade Relations" by Daniel T. Griswold, Ned Graham, Robert Kapp, and Nicholas Lardy (no. 5; July 19, 1999)

"The Steel 'Crisis' and the Costs of Protectionism" by Brink Lindsey, Daniel T. Griswold, and Aaron Lukas (no. 4; April 16, 1999)

"State and Local Sanctions Fail Constitutional Test" by David R. Schmahmann and James S. Finch (no. 3; August 6, 1998)

"Free Trade and Human Rights: The Moral Case for Engagement" by Robert A. Sirico (no. 2; July 17, 1998)

"The Blessings of Free Trade" by James K. Glassman (no. 1; May 1, 1998)

From the Cato Institute Briefing Papers Series

"The Myth of Superiority of American Encryption Products" by Henry B. Wolfe (no. 42; November 12, 1998)

CENTER FOR TRADE POLICY STUDIES

The mission of the Cato Institute's Center for Trade Policy Studies is to increase public understanding of the benefits of free trade and the costs of protectionism. The center publishes briefing papers, policy analyses, and books and hosts frequent policy forums and conferences on the full range of trade policy issues.

Scholars at the Cato trade policy center recognize that open markets mean wider choices and lower prices for businesses and consumers, as well as more vigorous competition that encourages greater productivity and innovation. Those benefits are available to any country that adopts free-trade policies; they are not contingent upon "fair trade" or a "level playing field" in other countries. Moreover, the case for free trade goes beyond economic efficiency. The freedom to trade is a basic human liberty, and its exercise across political borders unites people in peaceful cooperation and mutual prosperity.

The center is part of the Cato Institute, an independent policy research organization in Washington, D.C. The Cato Institute pursues a broad-based research program rooted in the traditional American principles of individual liberty and limited government.

For more information on the Center for Trade Policy Studies, visit www.freetrade.org.

Other Trade Studies from the Cato Institute

"Job Losses and Trade: A Reality Check" by Brink Lindsey, Trade Briefing Paper no. 19 (March 17, 2004)

"Trading Tyranny for Freedom: How Open Markets Till the Soil for Democracy" by Daniel T. Griswold, Trade Policy Analysis no. 26 (January 6, 2004)

"Threadbare Excuses: The Textile Industry's Campaign to Preserve Import Restraints" by Dan Ikenson, Trade Policy Analysis no. 25 (October 15, 2003)

"The Trade Front: Combating Terrorism with Open Markets" by Brink Lindsey, Trade Policy Analysis no. 24 (August 5, 2003)

"Free-Trade Agreements: Steppingstones to a More Open World" by Daniel T. Griswold, Trade Briefing Paper no. 18 (July 10, 2003)

"Ending the 'Chicken War': The Case for Abolishing the 25 Percent Truck Tariff" by Dan Ikenson, Trade Briefing Paper no. 17 (June 18, 2003)

"Grounds for Complaint? Understanding the 'Coffee Crisis'" by Brink Lindsey, Trade Briefing Paper no. 16 (May 6, 2003)