Order Code RL31733

Port and Maritime Security: Background and Issues for Congress

Updated December 15, 2004

John F. Frittelli
Specialist in Transportation
Resources, Science, and Industry Division

Port and Maritime Security: Background and Issues for Congress

Summary

The terrorist attacks of September 11, 2001 heightened awareness about the vulnerability to terrorist attack of all modes of transportation. Port security has emerged as a significant part of the overall debate on U.S. homeland security. The overarching issues for Congress are providing oversight on current port security programs and making or responding to proposals to improve port security.

The U.S. maritime system consists of more than 300 sea and river ports with more than 3,700 cargo and passenger terminals. However, a large fraction of maritime cargo is concentrated at a few major ports. Most ships calling at U.S. ports are foreign owned with foreign crews. Container ships have been the focus of much of the attention on seaport security because they are seen as vulnerable to terrorist infiltration. More than 6 million marine containers enter U.S. ports each year. While the Bureau of Customs and Border Protection (CBP) analyzes cargo information to target specific shipments for closer inspection, it physically inspects only a small fraction of the containers.

The Coast Guard and CBP are the federal agencies with the strongest presence in seaports. In response to September 11, 2001, the Coast Guard created the largest port-security operation since World War II. The Coast Guard has advanced its 24-hour Notice of Arrival (NOA) for ships to a 96-hour NOA. The NOA allows Coast Guard officials to select high risk ships for boarding upon their arrival at the entrance to a harbor. CBP has also advanced the timing of cargo information it receives from ocean carriers. Through the Container Security Initiative (CSI) program, CBP inspectors pre-screen U.S.-bound marine containers at foreign ports of loading.

To raise port security standards, Congress passed the Maritime Transportation Security Act of 2002 (P.L. 107-295) in November 2002. The focus of debate in Congress has been about whether current efforts to improve port security are adequate in addressing the threat. Significantly, one conclusion of *The 9/11 Commission Report* is that transportation security resources are not being "allocated to the greatest risks in a cost effective way.... Opportunities to do harm are as great, or greater, in maritime or surface transportation [than in aviation]. Initiatives to secure shipping containers have just begun...." While many agree that Coast Guard and CBP programs to address the threat are sound, they contend that these programs represent only a framework for building a maritime security regime, and that significant gaps in security still remain. The 9/11 Commission concluded that deployment of scanning technologies designed to screen containers that can be transported by plane, ship, truck, or rail is still years away. The Intelligence Reform and Terrorism Prevention Act of 2004 (S. 2845) contains provisions consistent with the recommendations of the 9/11 Commission for improving transportation security. This report will be updated periodically.

Key Policy Staff: Port and Maritime Security

Area of expertise	Name	Phone	E-mail
Transportation Security Admin.	John Frittelli	7-7033	jfrittelli@crs.loc.gov
Navy & Coast Guard	Ronald O'Rourke	7-7610	rorourke@crs.loc.gov
Customs & Border Protection	Jennifer Lake	7-0620	jlake@crs.loc.gov
Nuclear terrorism	Jonathan Medalia	7-7632	jmedalia@crs.loc.gov

Contents

Port and Maritime Security: Background and Issues for Congress

Introduction

This report[1] provides background information and discusses potential issues for Congress on the topic of port security, which has emerged as a significant part of the overall debate on U.S. homeland security.[2] The terrorist attacks of September 11, 2001 heightened awareness about the vulnerability to terrorist attack of U.S. ports and the ships in them. The issue for Congress is providing oversight on port security and proposals for improving it. Port security legislation can have significant implications for public safety, the war on terrorism, the U.S. and global economy, and federal, state, and local homeland security responsibilities and expenditures.

Background

Concerns for Port Security

Government leaders and security experts are worried that the maritime transportation system could be used by terrorists to smuggle personnel, weapons of mass destruction, or other dangerous materials into the United States. They are also concerned that ships in U.S. ports, particularly large commercial cargo ships or cruise ships, could be attacked by terrorists. Experts are concerned that a large-scale terrorist attack at a U.S. port could not only cause local death and damage, but also paralyze global maritime commerce.

James M. Loy, the former Commandant of the Coast Guard and now deputy secretary at the Department of Homeland Security, has described the nation's maritime transportation system as a natural gateway into America for asymmetrical military and terrorist threats.[3] The Commissioner of the Bureau of Customs and

---

[1] This report was prepared with assistance from Jennifer Lake, Jonathan Medalia, and Ronald O'Rourke.

[2] For other CRS products relating to maritime security, see CRS Report RS21293, *Terrorist Nuclear Attacks on Seaports: Threat and Response*; CRS Report RS21125, *Homeland Security: Coast Guard Operations — Background and Issues for Congress;* CRS Report RS21230, *Homeland Security: Navy Operations — Background and Issues for Congress*; CRS Report RS21997, *Port and Maritime Security: Potential for Terrorist Nuclear Attack Using Oil Tankers.*

[3] Admiral James M. Loy and Captain G. Ross, U.S. Coast Guard, "Global Trade: America's (continued...)

Border Protection, Robert Bonner, has stated that there is "virtually no security for what is the primary system to transport global trade."[4] Despite the progress that has been made in improving maritime security since September 11, a recent study by RAND Europe reports that "the maritime sector and specifically the container transport sector remain wide-open to the terrorist threat" and that "the system is perceived to be poorly defended against misuse and terrorism due to its global and open nature."[5] The 9/11 Commission reported that, "While commercial aviation remains a possible target, terrorists may turn their attention to other modes. Opportunities to do harm are as great, or greater, in maritime and surface transportation. Initiatives to secure shipping containers have just begun."[6]

Government officials and security experts were concerned about the security of U.S. ports even before the terrorist attacks of September 11, 2001. In the fall of 2000, the Interagency Commission on Crime and Security in U.S. Seaports noted the vulnerability of U.S. seaports to terrorism. The commission reported that a terrorist attack at a U.S. port could lead to significant loss of life, damage property and infrastructure, cause extensive environmental damage, and disrupt business and trade. The report noted that while the FBI then considered the threat of terrorist attacks on U.S. seaports to be low, their vulnerability to such attacks was high.[7] On July 20, 2001, Senator Hollings introduced S. 1214, the Maritime Transportation Security Act of 2001, a bill intended to strengthen U.S. port security.

The terrorist attacks of September 11, 2001, significantly heightened awareness about the vulnerability of U.S. ports and ships to a terrorist attack. In the months following the attacks, congressional committees held several hearings on the issue. In August 2002, the U.S. General Accounting Office (GAO) conducted field investigations of several U.S. seaports and found that ports are inherently vulnerable to terrorist attacks because of their size, easy accessibility by water and land, and the tremendous amount of cargo that is typically transferred through them.[8] And in October 2002, a security task force sponsored by the Council on Foreign Relations recommended that resources be reallocated to bolster sea and land transportation

---

[3] (...continued)
Achilles Heel," *Defense Horizons,* Feb. 2002. An asymmetrical threat is a military or terrorist method or tactic that does not mirror (i.e., is not symmetrical with) U.S. military capabilities. Asymmetrical attacks avoid an enemy's strengths and attack the enemy's weaknesses instead.

[4] Speech given at the Center for Strategic and International Studies dated Aug. 26, 2002, available at [http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/aug262002.xml] (viewed 10/07/04)

[5] RAND Europe, *Seacurity: Improving the Security of the Global Sea-Container Shipping System,* 2003.

[6] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States,* New York: W.W. Norton, 2004, p. 391.

[7] *Report of the Interagency Commission on Crime and Security in U.S. Seaports,* Fall 2000, p. 63.

[8] GAO, *Port Security, Nation Faces Formidable Challenges in Making New Initiatives Successful,* GAO-02-993T, Aug. 5, 2002.

security, asserting that the surface transportation system is far more vulnerable than the nation's aviation system.[9] In response to concerns for port security, on November 14, 2002, Congress passed S. 1214, as amended, the Maritime Transportation Security Act of 2002 (MTSA), and the President signed it into law as P.L. 107-295 on November 25, 2002. The Coast Guard and Maritime Transportation Act of 2004 was signed into law as P.L. 108-293 on August 9, 2004. Title VIII of the act adds specificity to some of the provisions in MTSA.

There is continuing debate about whether current efforts to improve port security are adequate in addressing the threat. Significantly, one conclusion of *The 9/11 Commission Report* is that transportation security resources are not being "allocated to the greatest risks in a cost effective way.... Opportunities to do harm are as great, or greater, in maritime or surface transportation [than in aviation]. Initiatives to secure shipping containers have just begun...."[10] While many agree that Coast Guard and CBP programs to address the threat are sound, they contend that these programs represent only a framework for building a maritime security regime, and that significant gaps in security still remain. The 9/11 Commission concluded that deployment of scanning technologies designed to screen containers that can be transported by plane, ship, truck, or rail is still years away.[11] The Intelligence Reform and Terrorism Prevention Act of 2004 (S. 2845) would implement the transportation security-related recommendations of the 9/11 Commission with respect to maritime transportation.

Features of the U.S. Maritime System

U.S. Ports. The U.S. maritime system includes more than 300 sea and river ports with more than 3,700 cargo and passenger terminals and more than 1,000 harbor channels spread along thousands of miles of coastline.[12]

Transportation firms tend to concentrate traffic through major cargo hubs because of the high cost of their infrastructure.[13] The top 50 ports in the United States account for about 90% of all cargo tonnage and 25 U.S. ports account for 98% of all container shipments.[14] Energy products are concentrated at particular ports.

---

[9] Report of an Independent Task Force Sponsored by the Council on Foreign Relations, *America Still Unprepared - America Still in Danger*, October 2002.

[10] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*, New York: W. W. Norton, 2004, p. 391.

[11] Ibid., pp. 391-92.

[12] For further information on the U.S. maritime system, see U.S. DOT, Maritime Admin., *An Assessment of the U.S. Marine Transportation System*, Sept. 1999. Available at [http://www.marad.dot.gov/].

[13] The U.S. Army Corps of Engineers' Navigation Data Center ranks U.S. ports by dollar value and tons of cargo imported and exported. See [http://www.iwr.usace.army.mil/ndc/].

[14] U.S. Congress, House of Representatives, Maritime Transportation Security Act of 2002, Conference Report, H.Rept. 107-777, p. 4.

For instance, almost one-quarter of California's imported crude oil is offloaded in one geographically confined area.[15]

Commercial Ships Using U.S. Ports. In 2001, approximately 5,400 commercial ships made more than 60,000 U.S. port calls. Most ships calling at U.S. ports are foreign owned and foreign crewed; less than 3% of U.S. overseas trade is carried on U.S.-flag vessels.[16]

Cargo Containers. Container ships are a growing segment of maritime commerce — and the focus of much of the attention on seaport security. Container ships carry stacks of marine containers loaded with a wide variety of goods. A large container ship can carry more than 3,000 containers, of which several hundred might be offloaded at a given port.

A marine container is similar to a truck trailer without wheels; standard sizes are 8 x 8 x 20 feet or 8 x 8 x 40 feet. Once offloaded from ships, they are transferred to rail cars or tractor-trailers or barges for inland transportation. Over-the-road weight regulations generally limit the cargo load of a 40 foot container to approximately 45,000 pounds. The estimated world inventory of containers is about 12 million. Container ships tend to carry higher-value cargo than other types of cargo ships. While they represent only 11% of annual tonnage, they account for 66% of the total value of U.S. maritime overseas trade. Containerized imports are dominated by consumer goods, such as clothing, shoes, electronics, and toys. U.S. automakers also import large quantities of parts in containers. Containerized exports are dominated by wastepaper, forest products, chemicals, and agricultural products.[17]

More than 6 million cargo containers enter U.S. sea ports each year. For comparison, about 13 million containers arrive by truck or rail from Canada and Mexico. CBP analyzes cargo manifest information for each container to decide which to target for closer inspection, based on such factors as origin, destination, shipper, and container contents. Only a small portion have their contents physically inspected by CBP. Physical inspection could include scanning the entire container with a sophisticated x-ray or gamma ray machine, unloading the contents of a container, or both.[18]

---

[15] *How Did This Happen?* ed. James F. Hoge, Jr. and Gideon Rose (New York: Public Affairs, 2001), p.186.

[16] "The Maritime Component," *Sea Power,* August 2001.

[17] For a list of the top importers and exporters of containerized marine cargo, see "Inside the Box," *Journal of Commerce,* Aug. 12-18, 2002, p. 20A.

[18] For further information on CBP's container inspection process, see CBP Fact Sheet: *The 5 Percent Myth vs. U.S. Customs and Border Protection Reality,* October 7, 2004.

Importance of the U.S. Maritime System

Economic Importance. Ships are the primary mode of transportation for world trade. Ships carry approximately 80% of world trade by volume.[19] The United States is the world's leading maritime trading nation, accounting for nearly 20% (measured in tons) of the annual world ocean-borne overseas trade. Ships carry more than 95% of the nation's non-North American trade by weight and 75% by value. Trade now accounts for 25% of U.S. Gross Domestic Product (GDP), up from 11% in 1970. Over the next two decades, the total volume of domestic and international trade is expected to double.

Given the importance of maritime trade to the U.S. and world economies, disruptions to that trade can have immediate and significant economic impacts.[20] By one estimate, the cost to the U.S. economy of the recent port closures on the West Coast due to a labor- management dispute was approximately $1 billion per day for the first five days, rising sharply thereafter.[21]

The container shipping system is designed for speed and efficiency. Transportation services are a critical component of the global, low-inventory (i.e., just-in-time) distribution model that many manufacturers have adopted. Most industries in the United States use some imported components from overseas suppliers. By bringing parts to a plant just before they are needed for assembly, manufacturers can save money on warehouse space and inventory carrying costs. Transport efficiencies permit warehouse requirements to be minimized. Lean inventories in turn have contributed to business productivity. From 1980 to 2000, according to one study, business logistics costs dropped from 16.1% of U.S. GDP to 10.1%.[22]

Given the dependence of the United States and the global economy on a highly efficient maritime transportation system, many experts acknowledge that slowing the flow of trade to inspect all inbound containers, or at least a statistically significant random selection would be, in the words of James M. Loy, former Coast Guard Commandant and now deputy secretary at the Department of Homeland Security, "economically intolerable."[23] Supply chain analysts are concerned that increased security-related delay at seaports could threaten the efficiency gains achieved in

---

[19] United Nations Conference on Trade and Development (UNCTAD), *Review of Maritime Transport 2002*.

[20] For further information, see OECD, *Security in Maritime Transport: Risk Factors and Economic Impact,* Maritime Transport Committee, July 2003.

[21] Report of an Independent Task Force Sponsored by the Council on Foreign Relations, *America Still Unprepared — America Still in Danger,* October 2002, p. 23.

[22] Michael Wolfe, North River Consulting Group, *Freight Transportation Security and Productivity,* report prepared for U.S. DOT, EU/US Forum on Intermodal Freight Transport, Apr. 11-13, 2001.

[23] Admiral James M. Loy and Captain Robert G. Ross, "Global Trade, America's Achilles Heel," *Defense Horizons,* Feb. 2002.

inventory management over the past two decades by forcing companies to hold larger inventories.

Enhanced security has benefits as well as costs. Many experts see economic benefits to tighter control over maritime commerce. Resources put towards seaport security can also reduce cargo theft, narcotic and migrant smuggling, trade law violations, the accidental introduction of invasive species, and the cost of cargo insurance. Improved planning for responding to a terrorist attack at a seaport could also improve responses to other emergencies, such as natural disasters or transportation accidents. New technologies intended to convert the sea container into a "smart box," such as electronic seals, sensors, or tracking devices, could also improve shipment integrity, help carriers improve their equipment utilization, and help cargo owners track their shipments. In response to the terrorist threat, the CBP has accelerated development of its new information management system, the Automated Commercial Environment (ACE). This system will assist CBP in evaluating cargo manifest information for high risk shipments but will also speed the customs filing process for U.S. importers.[24]

National Security Importance. In addition to its economic significance, the marine transportation system is vital for national security. The Departments of Defense and Transportation have designated 17 U.S. seaports as strategic because they are necessary for use by DOD in the event of a major military deployment. Thirteen of these ports are commercial seaports. During Desert Storm, 90% of all military equipment and supplies were shipped from U.S. strategic ports. The deployment required over 312 vessels from 18 commercial and military ports in the United States. As the GAO has reported, "If the strategic ports (or the ships carrying military supplies) were attacked, not only could massive civilian casualties be sustained, but DOD could also lose precious cargo and time and be forced to rely heavily on its overburdened airlift capabilities."[25]

Port Security Threat Scenarios

Security experts are concerned about a variety of terrorist threat scenarios at U.S. ports. Among other things, they are concerned that terrorists could:

- use commercial cargo containers to smuggle terrorists, nuclear, chemical, or biological weapons, components thereof, or other dangerous materials into the United States;

- seize control of a large commercial cargo ship and use it as a collision weapon for destroying a bridge or refinery located on the waterfront;

---

[24] For further information on ACE, see [http://www.cbp.gov/xp/cgov/toolbox/about/modernization/] (viewed 12/4/03).

[25] GAO, *Combating Terrorism, Actions Needed to Improve Force Protection for DOD Deployments through Domestic Seaports*, GAO-03-15, Oct. 2002.

- sink a large commercial cargo ship in a major shipping channel, thereby blocking all traffic to and from the port;

- attack a large ship carrying a volatile fuel (such as liquefied natural gas) and detonate the fuel so as to cause a massive in-port explosion;

- attack an oil tanker in a port or at an offshore discharge facility[26] so as to disrupt the world oil trade and cause large-scale environmental damage;

- seize control of a ferry (which can carry hundreds of passengers) or a cruise ship (which can carry more than 3,000 passengers, of whom about 90% are usually U.S. citizens) and threaten the deaths of the passengers if a demand is not met;

- attack U.S. Navy ships in an attempt to kill U.S. military personnel, damage or destroy a valuable U.S. military asset, and (in the case of nuclear-powered ships) cause a radiological release.

- use land around a port to stage attacks on bridges, refineries located on the waterfront, or other port facilities.

Some of these scenarios (or similar ones) have already come to pass elsewhere. For example, in October 2002, the French oil tanker *Limberg* appears to have been attacked by a bomb-laden boat off the coast of Yemen, killing one crewman aboard the tanker, damaging the ship, and causing an oil spill.[27] In October 2001, Italian authorities arrested on terrorism charges an Egyptian-born Canadian citizen found with high-tech equipment (including a satellite phone and a computer) and other personal possessions in a cargo container in an Italian port.[28] In October 2000, the U.S. Navy destroyer Cole was attacked by a bomb-laden boat during a refueling stop in the harbor of Aden, Yemen, killing 17 sailors, injuring 39 others, and causing damage to the ship that cost about $250 million to repair.[29] In 1985, terrorists seized the cruise ship *Achille Lauro* in the Mediterranean and held its passengers hostage, killing one of them.

---

[26] In an offshore "lightering" zone, a very large crude carrier (VLCC) or "supertanker" transfers part of its cargo to a smaller shuttle tanker that delivers the crude oil to the tank farm or refinery onshore. There are also offshore oil ports where a tanker discharges its cargo through a submerged pipeline that carries the cargo along the seabed to the onshore terminal.

[27] "Ships as Terrorist Targets," *American Shipper,* Nov. 2002, p.59.

[28] His lawyers argued that he was a Maronite Christian fleeing religious discrimination and personal legal problems in Egypt who was shipping his possessions to Canada and planned to fly from Rome to Montreal. (He was also carrying a plane ticket.) Charges against him were dropped and he was ordered freed from jail in mid-November 2001. (Italian Court Frees Canadian Suspect. *Toronto Star*, November 16, 2002.)

[29] CRS Report RS20721, *Terrorist Attack on U.S.S. Cole: Background and Issues for Congress.*

Much concern has focused on the threat that a sea container could be used to smuggle a nuclear weapon into the United States. Experts are concerned that if a nuclear weapon in a container aboard a ship in port is detonated, it could not only kill tens of thousands of people and cause massive destruction, but could also paralyze the movement of cargo containers globally, thereby shutting down world trade.[30]

Port and Ship Vulnerabilities to Terrorist Attack

Port Facilities. Port areas and ships in ports have many vulnerabilities to potential terrorist attack. Port areas have very large landside perimeters to secure, giving terrorists many potential landside points of entry. Some ports are located immediately adjacent to built-up urban areas, giving terrorists places to hide while approaching or escaping from port areas. Large numbers of trucks move in and out of ports, making it possible for terrorists to use a truck to bring themselves and their weapons into a port. Many ports harbor fishing and recreational boats that terrorists could use to mask their approach to a target ship.

Ships. Commercial cargo ships at pier or at anchorage in harbor are stationary, and those moving through port do so at slow speeds, making them easy to intercept by a fast-moving boat. Commercial cargo ships are generally unarmed and have very small crews, making them vulnerable to seizure by a small group of armed people, as proven by modern-day pirates. In the 1990s, the number of reported attacks on cargo ships by pirates tripled.[31] Most pirate attacks occur while the ship is in port. Although most attacks occur in Southeast Asian waters on foreign-flag freighters, U.S. shippers are likely to be among the owners of cargo onboard. It can also be noted that some experts believe there is a link between piracy and terrorism — that the goal of some acts of piracy may be to raise money to finance terrorist operations. The *Financial Times* has reported an incident where a chemical tanker in the south Pacific was boarded by pirates who practiced steering the vessel at varying speeds for several hours.[32]

The lack of transparency in ship registration has been a longstanding concern. An Organization for Economic Cooperation and Development (OECD) study on the ownership and control of ships reports that:

> Not only does perfect transparency not exist, but in fact anonymity seems to be the rule rather than the exception, and not only is it permitted, but in many cases positively encouraged. This enables terrorists and would be terrorists to remain intimately involved in the operation of their vessels, while maintaining totally

---

[30] U.S. Department of the Treasury, Customs Service. Robert Bonner, U.S. Customs Commissioner, Speech Before the Center for Strategic and International Studies, Washington, D.C., January 17, 2002. [http://www.cbp.gov/xp/cgov/newsroom/commissioner/speeches_statements/archives/jan172002.xml].

[31] U.S. DOT, *Surface Transportation Security: Vulnerabilities and Developing Solutions*, n.d., n.p.

[32] "The Maritime Threat from Al Qaeda," *Financial Times*, October 20, 2003.

> hidden, through the use of relatively simple mechanisms that are readily available and legally tolerated in almost all jurisdictions.[33]

Unscrupulous ship owners are known to mask their identity by re-registering their vessels under fictitious corporate names and renaming and repainting their ships. Shipowners can register their vessels in "flag of convenience" countries which may have lax regulations and require little information from the applicants. According to press reports, U.S. intelligence officials believe they have identified 15 cargo ships that have links to al Qaeda.[34]

Container Shipments. The complexity of the process for completing containerized shipments makes it more difficult to ensure the integrity of this type of cargo.[35] Unlike other cargo ships whose loading process occurs at the port and whose cargo is often owned by a single company, container ships carry cargo from hundreds of companies and the containers are loaded away from the port at individual company warehouses. A typical single container shipment may involve a multitude of parties and generate 30 to 40 documents. A single container could also carry cargo for several customers, thus multiplying the number of parties and documents involved. The parties involved in a shipment usually include the exporter, the importer, a freight forwarder, a customs broker, a customs inspector, inland transportation provider(s) (which may include more than one trucker or railroad), the port operators, possibly a feeder ship, and the ocean carrier. Each transfer of the container from one party to the next is a point of vulnerability in the supply chain. The security of each transfer facility and the trustworthiness of each company is therefore critical in the overall security of the shipment. It is also important to keep in mind that not all U.S.-bound containers arrive at U.S. ports. Half of the containers discharged at the Port of Montreal, for instance, move by truck or rail for cities in the northeastern or mid-western United States.[36] Also, many containers that enter U.S. waters are bound for other nations.

Maritime Crimes. Security experts warn that terrorists attempting to use a container to smuggle a weapon of mass destruction or components thereof into the United States could purchase a known exporter with a long and trustworthy shipping record. Drug smugglers have been known to employ this strategy to disguise their contraband in otherwise legitimate cargo. While both the Coast Guard and CBP are experienced in the marine environment with the "war on drugs," they recognize that terrorism is a different kind of threat. Among other things, drug smugglers are often interested in finding a smuggling method that can be used over and over to make

---

[33] OECD, *Ownership and Control of Ships,* Maritime Transport Committee, March 2003, p. 5.

[34] See "15 Freighters Believed to Be Linked to al Qaeda," *Washington Post,* Dec. 31, 2002, p. A1. Also, "Terrorism - Bin Laden Group Shipping Interests Probed," *Lloyd's List,* Sept. 28, 2001.

[35] See, Arun Chatterjee, *An Overview of Security Issues Involving Marine Containers and Ports,* proceedings of the 2003 Transportation Research Board Annual Meeting, available on CD-ROM.

[36] Hoge and Rose, ed. *How Did This Happen?* p. 188.

multiple shipments. This permits the Coast Guard and CBP to look for certain patterns of operation among drug smugglers. Terrorists, on the other hand, are more likely to be interested in using a particular method of attack only once, to carry out a particular terrorist operation. This makes the tactic of looking for patterns of operation potentially much less useful. Another difference concerns the potential consequences of failure to detect and intercept: Given the tremendous amount of cargo arriving at seaports, the mission of interdicting illegal drugs or a weapon of mass destruction is often described as searching for the needle in the haystack. In the case of the weapon of mass destruction, however, the potential consequence of not finding the so-called needle is much greater.

The incidence of other shipping-related crimes also attests to the challenges faced in improving port security. The National Cargo Security Council estimates that cargo theft domestically ranges between $10 billion and $15 billion annually.[37] The FBI believes much of this theft occurs in or near seaports.[38] Identifying where cargo theft occurs in the transportation system may help identify where terrorist infiltration could occur.

Government Authorities at Seaports

Port Governance and Financing. In considering how to enhance seaport security, it is important to know how they are governed and operated. The governing structure of ports varies from place to place. While the federal government has jurisdiction over interstate and foreign commerce and designated federal waterway channels, state or local governments have ownership over ports. There are ports which are part of state government and others which are part of city government. The Port Authority of New York and New Jersey and the Delaware River Port Authority are examples of bi-state or regional port agencies.

Ports can be a subsidiary of a public agency but may be structured to act as a private sector corporation. Most ports are "landlord ports," which means the port provides the basic services and infrastructure but the tenant, such as a terminal operator, performs most of the activity. "Operating ports" both generate and carry out most of the activity at the port. In addition to city law enforcement personnel, some port authorities also have their own police forces.

Depending on how they are structured, ports finance infrastructure improvements through a variety of means. Some may levy taxes, if they are granted this authority. Ports may also pay for infrastructure with the general funds they receive from the governments they are a part of, from operating revenues, general obligation bonds, revenue bonds, trust fund monies, or loan guarantees. Most ports generally break even or are minimally profitable.[39]

---

[37] "Executive Viewpoint, Joe M. Baker, Jr. Exec. Director, NCSC," *Journal of Commerce,* May 8, 2002.

[38] "Cargo Crime Bill Hit," *Traffic World,* Oct. 9, 2000.

[39] U.S. DOT, Maritime Administration, *Public Port Finance Survey for FY1999,* Jan. 2001.

Federal Agencies Involved in Port Security. Federal agencies involved in port security include the Coast Guard, the Bureau of Customs and Border Protection (CBP), and the Transportation Security Agency (TSA), all of which are housed in the Department of Homeland Security (DHS), and the Maritime Administration (MARAD). The Coast Guard and CBP are the two federal agencies with the strongest presence at seaports.

Coast Guard. The Coast Guard is the nation's principal maritime law enforcement authority and the lead federal agency for the maritime component of homeland security, including port security.[40] Among other things, the Coast Guard is responsible for evaluating, boarding, and inspecting commercial ships as they approach U.S. waters, for countering terrorist threats in U.S. ports, and for helping to protect U.S. Navy ships in U.S. ports. A high-ranking Coast Guard officer in each port area serves as the Captain of the Port (COTP), who is lead federal official responsible for the security and safety of the vessels and waterways in his or her geographic zone. Under the terms of the Ports and Waterways Safety Act of 1972 (P.L. 92-340) and the recently enacted Maritime Transportation Security Act of 2002, the Coast Guard has responsibility to protect vessels and harbors from subversive acts.

Bureau of Customs and Border Protection. The Bureau of Customs and Border Protection (CBP) is the federal agency with principal responsibility for inspecting cargoes, including cargo containers, that commercial ships bring into U.S. ports and for the examination and inspection of ship crews and cruise ship passengers for ships arriving in U.S. ports from any foreign port. Prior to the establishment of the CBP, customs and immigration functions at U.S. borders were conducted separately by the Department of the Treasury's U.S. Customs Service and the Department of Justice's Immigration and Naturalization Service.

Transportation Security Administration. TSA is an agency created by the Aviation and Transportation Security Act of 2001 (P.L. 107-71). Initially, its focus was the security of air transportation but it is responsible for the security of all modes of transportation, cargo and passenger.

Maritime Administration. MARAD, which is part of the Department of Transportation (DOT), is a civilian agency that supports the U.S. commercial maritime industry. MARAD publishes regular Maritime Security Reports and a national planning guide on port security. MTSA requires MARAD to publish a revised version of its national planning guide on port security.

---

[40] The Navy and the Coast Guard agree that the Coast Guard is the lead federal agency for the maritime component of homeland security, and that the Navy's role is to support the Coast Guard in areas where the Coast Guard's capabilities are limited or lacking, such as air defense or antisubmarine warfare. For more on the Navy's role in homeland security, see CRS Report RS21230, *Homeland Security: Navy Operations — Background and Issues for Congress*, by Ronald O'Rourke.

Port Security Initiatives by Federal Agencies

Coast Guard. In response to the terrorist attacks of September 11, 2001, the Coast Guard created the largest port-security operation since World War II. Coast Guard cutters and aircraft were diverted from more distant operating areas to patrol U.S. ports and coastal waters. The Coast Guard began to maintain security zones around waterside facilities, Navy ships, and cruise and cargo ships entering or leaving port. Coast Guard port security teams began to inspect certain high-interest vessels, and Coast Guard sea marshals began escorting certain ships transiting the harbor.

To counter the terrorist threat, the Coast Guard and CBP have sought to improve the quality and advance the timing of information submitted to them by shippers and carriers so that they can better evaluate the terrorist risk of ships, cargo, or crew bound for the United States. By increasing their knowledge of the various parties in the marine environment it is hoped that federal authorities will be better able to separate the bad from the good without impeding the flow of legitimate commerce.

In support of this goal, the Coast Guard has instituted new reporting requirements for ships entering and leaving U.S. harbors. The former 24-hour advance Notice of Arrival (NOA) has been extended to a 96-hour NOA. The NOA includes detailed information on the crew, passengers, cargo, and the vessel itself.

The Coast Guard has also developed the concept of maritime domain awareness (MDA). MDA involves fusing intelligence information with information from public, private, commercial, and international sources to provide a more complete picture of potential maritime security threats. The Coast Guard will use this picture to support a risk-management approach to preventing or mitigating terrorist threats through the use of actionable knowledge.[41]

On October 22, 2003 the Coast Guard issued final rules implementing MTSA.[42] These regulations became effective on November 21, 2003.

Bureau of Customs and Border Protection. Among the programs CBP has initiated to counter the terrorist threat are the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). CSI is a series of bilateral, reciprocal agreements that, among other things, allow CBP personnel at selected foreign ports to pre-screen U.S.-bound containers. As of July 2004, CSI is operational at 20 overseas ports. In order to give inspectors the data and time they need to pre-screen containers, CBP issued a new rule requiring that information about an ocean shipment be transmitted to CBP 24 hours *before* the cargo is loaded at a foreign port onto a U.S.-bound vessel. Previously, ocean carriers did not submit this information until the ship arrived at a U.S. port. CBP is also requiring more comprehensive and specific cargo information so it can more efficiently evaluate individual container shipments for risks of terrorism. The use of general cargo

---

[41] For further information on the Coast Guard as it relates to homeland security, see CRS Report RS21125, *Homeland Security: Coast Guard Operations — Background and Issues for Congress* by Ronald O'Rourke.

[42] See 68 Federal Register 60447 (Oct. 22, 2002).

descriptions such as "freight of all kinds," "general cargo," or "chemicals" will no longer be accepted. More detailed descriptions are intended to help speed up non-intrusive inspections of high risk containers by reducing the number of containers inspectors need to unload for closer examination. The rationale of CSI is that a nuclear weapon or a radiological "dirty bomb"[43] that enters a U.S. port could be detonated, before the ship is inspected.[44]

C-TPAT, initiated in April 2002, offers importers expedited processing of cargo if they comply with CBP guidelines for securing their entire supply chain. Businesses that sign up for the program are required, among other things, to conduct a comprehensive self-assessment of their supply chain and submit a completed questionnaire to CBP that describes their current security practices. If CBP certifies an applicant, they may benefit from a reduced number of cargo inspections, thus reducing the risk of shipment delay. Over 4,500 companies have agreed to participate in the program.

Transportation Security Administration. The Transportation Security Administration in conjunction with CBP is conducting the Operation Safe Commerce (OSC) pilot project.[45] The goal of OSC is to verify the contents of containers at their point of loading, ensure the physical integrity of containers in transit, and track their movement through each mode of transport from origin to final destination. Container tracking is a key area of debate on cargo security. Various "smart container" devices are being developed that would provide real-time location information and container tampering notification. The challenge is developing a device that can withstand the harsh ocean environment, be relatively inexpensive, and reliable enough not to trigger false alarms. TSA is also field-testing a Transportation Worker Identification Credential (TWIC) for workers in all modes of transportation that will be used to control access to secure areas of cargo and passenger facilities. The agency has developed a "Maritime Self-Assessment Risk Module" to assist port terminal and vessel owners in developing their security plans as required by MTSA.

Maritime Administration. MARAD, along with the Coast Guard, CBP, and TSA, is part of the Container Working Group which has made classified recommendations on how best to ensure the security of marine container transportation. MARAD has also developed a curriculum for training maritime security personnel.

International Institutions. In June 2002, the Group of Eight Nations identified the IMO and the World Customs Organization (WCO) as two institutions that should develop global initiatives to improve maritime security. However, the

---

[43] A dirty bomb is a conventional explosive device with radioactive material wrapped around it. Detonating the device disperses the radioactive material, contaminating the area with radioactivity that can be difficult to clean. Dirty bombs are also known as radiological dispersion devices. For further information, see CRS Report RS21528, *Terrorist 'Dirty Bombs': A Brief Primer.*

[44] See also, GAO, *Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T, March 31, 2004.

[45] 67 Federal Register 70110-70112 (Nov. 2, 2002).

authority of the IMO and WCO stops at the borders of countries. Individual governments must enforce the standards and conventions developed by these institutions in order for them to have any real authority.

At its December 2002 conference, the IMO adopted a new chapter to the Safety of Life at Sea (SOLAS) Convention entitled International Ship and Port Facility Security (ISPS) Code.[46] The code contains both mandates and voluntary measures to improve maritime security. IMO member governments had until July 1, 2004 to implement the new regulations. The code largely parallels the requirements called for in MTSA.[47]

The World Customs Organization is a Brussels-based entity that has been working towards simplifying and harmonizing customs procedures to improve the efficiency of cross-border trade.[48] Currently, 161 countries accounting for 97% of world trade are members of the WCO. In June 2002, the WCO created a task force to draft a "Resolution on Security and Facilitation of the International Supply Chain" which they completed in June 2003. The task force includes 50 countries and 25 organizations. The objective of the task force is to standardize a set of data elements needed to identify high risk cargo and to exchange that information between an exporting and an importing customs administration.

Recent Law on Port Security

The bill creating the new Department of Homeland Security (DHS), was passed by the Senate on November 19, 2002 and by the House on November 22, 2002, and signed into law as P.L. 107-296 on November 25, 2002. The DHS incorporates the Coast Guard, the former Customs Service, and TSA, among others.[49]

The Maritime Transportation Security Act of 2002 was passed by Congress on November 14, 2002 and signed into law as P.L. 107-295 on November 25, 2002. The act creates a U.S. maritime security system and requires federal agencies, ports, and vessel owners to take numerous steps to upgrade security. The act requires the Coast Guard to develop national and regional area maritime transportation security plans. It requires ports, waterfront terminals, and certain types of vessels to develop security and incident response plans with approval from the Coast Guard. The act authorizes CBP to require that cargo manifest information for inbound or outbound shipments be provided to the agency electronically prior to the arrival or departure of the cargo. This information may be shared with other appropriate federal agencies. The legislation calls on the Department of Transportation to determine the level of

---

[46] For further information about the code, see [http://www.imo.org/home.asp].

[47] For further information on meeting this deadline, see GAO, *Maritime Security: Substantial Work Remains to Translate New Planning Requirements into Effective Port Security,* GAO-04-838, June 2004.

[48] For further information about the WCO and trade security, see [http://www.wcoomd.org/ie/En/en.html].

[49] For further information, see CRS Report RL31549, *Department of Homeland Security: Consolidation of Border and Transportation Security Agencies,* by William J. Krouse.

funding needed for a grant program that will finance security upgrades. The act also authorizes $90 million in grants for research and development in improving cargo inspection, detecting nuclear materials, and improving the physical security of marine containers. A dispute over how to pay for the cost of enhancing port security was resolved by eliminating controversial user fee provisions from the conference report (funding issues are discussed further below).

The Trade Act of 2002 (P.L. 107-210) was enacted into law on August 6, 2002. Section 343 provides authority to CBP to issue regulations requiring the electronic transmission of cargo information to CBP prior to the shipments' exportation or importation into the United States.

The Coast Guard and Maritime Transportation Act of 2004 was signed into law as P.L. 108-293 on August 9, 2004. Title VIII of the act contains a number of provisions related to maritime security, many of which add specificity to provisions in MTSA. Among other things, the act requires the DHS to submit a plan to Congress implementing a maritime intelligence system (section 803); it requires the DHS to submit a plan for a maritime security grant program, including recommendations on how funds should be allocated (section 804); it requires the Coast Guard to report on the implementation and use of joint operational centers at certain U.S. ports (section 807); it requires the DOT to investigate and examine sensors that are able to track marine containers throughout their supply chain and detect hazardous and radioactive materials within the containers (section 808); it requires the DHS to report on the costs of vessel and container inspections, and a plan for implementing secure systems of transportation, including the need for and feasibility to inspect and monitor intermodal shipping containers within the United States (section 809).

The week of December 6, 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (S. 2845) which, at the time of this writing, is expected to be signed into law. The Act imposes an urgency on DHS's efforts in strengthening maritime security by imposing deadlines on the agency in planning and carrying out certain maritime security activities that were called for in MTSA. This includes a deadline of April 1, 2005 for completion of a national maritime security plan; a deadline of December 31, 2004 for completion of facility and vessel vulnerability assessments; and deadlines for a deployment plan for TWIC, a status report on standards for seafarer identification, and a status report on establishing performance standards for container seals and locks. The Act also requires DHS to create a terrorism "watch list" for passengers and crew aboard cruise ships.

Issues for Congress

The challenge of port security raises several potential issues for Congress. Some Members of Congress, who have introduced their own versions of maritime security legislation, are concerned that MTSA does not go far enough in its requirements. In addition to considering further port security legislation, Congress is debating whether the federal government is providing enough funds to port

authorities and border agencies for improving port security. Congress is also considering how to pay for port security.

Addressing the Threat

A major concern for Congress is assessing whether the Nation is addressing the threat to maritime security with enough urgency. Despite the progress that has been made in strengthening port security thus far, many security officials still describe seaports as "wide open" and "very vulnerable" to terrorist attack.[50] Seaports, along with air cargo, general aviation, and mass transit were identified in a recent GAO report as the "major vulnerabilities" remaining in the nation's transportation system.[51] The GAO found that "an effective port security environment may be many years away." While many agree that CSI, C-TPAT, OSC, and MDA, are sound strategies for addressing the threat, they contend that these programs represent only a framework for building a maritime security regime, and that significant gaps in security still remain. In the words of one security expert,[52]

> Right now, none of these initiatives has changed the intermodal transportation environment sufficiently to fundamentally reduce the vulnerability of the cargo container as a means of terrorism. However, all are important stepping-off points for building an effective risk management approach to container security — a foundation that simply did not exist prior to September 11, 2001.

In its oversight role, Congress is examining the effectiveness of these programs in addressing the terrorist threat, whether they are proceeding at sufficient pace, and whether enough resources are being provided to implement these and other security initiatives.

Some observers and Members of Congress are concerned that initiatives to fill gaps in port security are not proceeding at a sufficient pace. Some have criticized MTSA because it does not establish firm deadlines, similar to those contained in airport security legislation, for implementing certain uniform security measures at all seaports. TSA's program to credential all transportation workers and its effort to develop a "smart-box" to ensure the integrity of container shipments has also been criticized for moving forward too slowly. Some argue that the security funding provided to seaports, especially when compared to the amount provided to airports, is woefully inadequate.

Others argue that current efforts to improve port security are proceeding at an unprecedented pace. They note that the IMO, with leadership from the U.S. Coast Guard, agreed to new international port security measures within a year. They also note that the Coast Guard issued final rules implementing MTSA within a year after becoming law. During Operation Liberty Shield, (March 17, 2003 through April 16, 2003) the Coast Guard and CBP demonstrated their ability to rapidly intensify port

---

[50] "Safe Harbors?" *Wall Street Journal,* April 21, 2003, p.B1.

[51] GAO, *Transportation Security, Post September 11th Initiatives and Long-Term Challenges,* April 1, 2003, GAO-03-616T.

[52] Stephen Flynn, "On The Record," *Government Executive Magazine,* October 1, 2003.

security operations by increasing ship and cargo inspections, increasing air and surface patrols, escorting more ships through harbors, and other activities. For further information on Operation Liberty Shield, see CRS Report RS21475, *Operation Liberty Shield: Border, Transportation, and Domestic Security*.

Funding Port Security

According to many, the unresolved debate over how to pay for port security is stalling efforts to improve port security. The debate is over whether port security should be paid for with federal revenues, by state and local governments, by the maritime industry, or by a cost sharing arrangement among all of the above. The Coast Guard roughly estimates the cost of implementing the new IMO security code and the security provisions in MTSA to be approximately $1.5 billion for the first year and $7.3 billion over the succeeding decade.[53] Congress has provided over $650 million through FY2005 in direct federal grants to ports to improve their physical and operational security. This is in addition to the budgets of the Coast Guard, Bureau of Customs and Border Protection, TSA, and other federal agencies involved in port security.[54] Advocates for more spending argue that the federal funds provided to port authorities thus far are woefully inadequate, particularly when compared to airports. Skeptics of additional spending argue that taxpayers should not provide funds to large and profitable corporations to secure infrastructure that is in their own financial interest to do so.

Sources of Funds. A dispute over how to finance security requirements arose during the conference committee on MTSA. Senator Hollings proposed creating a system of user fees on ship cargo as a means of generating funds for port security upgrades required in the legislation. Other conferees opposed this proposal, calling the user fees a tax. Some policymakers contend that without providing a funding source, the act amounts to an unfunded mandate.

Port authorities, ocean carriers, and shippers argue that port security is a national concern and therefore the federal government should finance it through general revenues. Others argue that the maritime industry should finance port security through user fees because it is a direct beneficiary of improved security as it reduces cargo theft and other economic damages.[55]

Proponents of user fees contend that user surcharges are an effective means of ensuring improved security because they would provide a more secure and predictable source of funding than annual appropriations. They propose that a port security trust fund be created in a manner that prevents the user fees from being spent on anything other than port security. If such a port security trust fund were created,

---

[53] See 68 Federal Register 60464 (Oct. 22, 2002).

[54] See CRS Report RL32061, *Border and Transportation Security: Budget for FY2003 and FY2004.*

[55] Representative Dana Rohrabacher introduced an amendment to H.R. 2557 that would allow ports to impose a per-container fee to pay for port security. Unlike Senator Hollings's user fee proposal, the fund would be administered locally by individual ports.

they argue, port security would not have to compete with other funding priorities in the annual appropriations process. Some economists contend that a user fee system is also more efficient than direct subsidies because the users of the service being provided (in this case port security) are likely to demand that policymakers spend the funds in the most productive manner.

Allocating Resources. An issue of likely interest to Congress is how to allocate resources appropriately to the various ports. Maximum security is prohibitively expensive. Therefore, it is important to properly identify specific security areas that have the greatest vulnerability and apportion funds accordingly. Criteria could include a port's relative economic importance and its proximity to an urban or sensitive area. The 9/11 Commission criticized the TSA for lacking a strategic plan for systematically analyzing transportation assets, risks, costs, and benefits in order to allocate limited resources in the most cost-effective way.[56] (See also the last section of this report for a discussion of H.R. 10 and S. 2845).

Resources for Foreign Ports. In addition to funding security at U.S. ports, there is also the issue of finding resources for improving security at foreign ports, especially in developing countries that may not be able to afford the technology to improve their ports' security. The IMO's recent adoption of new security measures includes a statement inviting the Secretary General of the IMO to give early consideration to establishing a "Maritime Security Trust Fund" for the purpose of providing financial support in developing countries for strengthening their maritime security infrastructure.[57]

Balancing Security and Commerce

Security experts argue that perfect maritime security can only be achieved by shutting down the transportation system. As one observer stated, "a harbor without ships is safe, but that is not what harbors are built for."[58] The issue for Congress is how to increase port security to desired levels while minimizing the economic impacts associated with impeding the maritime trade system. When security experts speak of significant gaps still remaining in maritime security, they are often referring to the credibility problems associated with the container loading process overseas and the true identity of ships and their crew on the high seas.

Point of Origin Cargo Security. A major area of concern is ensuring the integrity of cargo as it begins its transit to the United States from its overseas origin. Point of origin security is necessary because inspecting cargo on the high seas is practically impossible and inspecting cargo upon its arrival at a U.S. port could be too late to prevent a terrorist event. Ensuring that the container was not stuffed with illegitimate cargo at the overseas factory, that the loaded container was not tampered

---

[56] *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (New York: W.W. Norton, 2004), p. 391.

[57] For further information, see [http://www.imo.org/home.asp].

[58] "Port Shutdown for Terrorist Incidents Could Cost Billions, Drill Shows," *CQ Homeland Security*, Dec. 5, 2002.

with while trucked to the port of loading, and ensuring that the cargo information reported to CBP is not fraudulent are all critical challenges in supply chain security. Congress is examining the effectiveness of C-TPAT, CSI, and OSC in ensuring the integrity of U.S. bound cargo at its overseas point of origin.[59] Finding the right balance between improving cargo security to desired levels without unduly impeding the legitimate flow of commerce is a difficult issue.

Congress may review whether the cargo manifest is the best document to use in flagging high risk cargo. The fundamental problem with cargo information is that it is only as trustworthy as the person providing it. Some have suggested that cargo manifests, which traditionally have been utilized for commercial compliance, may not be the best tool to use for national security purposes. Some former maritime officials have suggested that CBP could strengthen its screening process by utilizing other business documentation.[60] Such documentation could include a purchase order, a shipper's letter of instruction, commercial invoice, letter of credit, or certificate of origin. These documents are typically generated before the shipment of the cargo begins. They are generally part of everyday import and export transactions and some believe they would provide richer and more trustworthy data for flagging high risk shipments.[61]

Vessels Under Foreign Ownership and Control. There is no single sovereign power that regulates international shipping. MTSA requires the Coast Guard to report on foreign-flag vessels calling at U.S. ports, specifically those vessels with murky ownership histories, and to report on actions taken to improve the transparency of vessel registration procedures (section 112). In December 2002, as mentioned above, the IMO adopted more stringent international standards for the security of vessels and ports.

Congress is likely to examine the effectiveness of Coast Guard and international efforts at raising the security level of ship operators. Skeptics contend that the new IMO regulations mostly offer the illusion of increased security. They contend that "flag of convenience" countries lack the resolve to enforce these standards and that the compliance documentation is too easy to manipulate in order to appear as legitimate operators.[62] While the United States enforces its standards when the Coast

---

[59] See Senate Governmental Affairs Committee, Letter to Under Secretary for Border and Transportation Security, dated October 28, 2003, regarding point of origin security measures. Available at [http://govt-aff.senate.gov/], viewed on 11/10/03. See also GAO, *Container Security: Expansion of Key Customs Programs Will Require Greater Attention to Critical Success Factors,* July 2003, GAO-03-770.

[60] Testimony of Robert Quartel, former member of the Federal Maritime Commission, U.S. Congress, Senate hearing on *Securing Our Ports against Terror: Technology, Resources and Homeland Defense,* Subcommittee on Technology, Terrorism and Government Information, Feb. 26, 2002; and testimony of Stephen Flynn, Council on Foreign Relations, Senate hearing on *Cargo Containers: The Next Terrorist Target?,* Committee on Government Affairs, March 20, 2003.

[61] See "Pushing the Border . . . Out," *Journal of Commerce,* Feb. 18, 2002.

[62] See, for example, William Langewiesche, "Anarchy at Sea," *Atlantic Monthly,* Sept. 2003, p. 50.

Guard selects arriving ships for boarding, their burden is greater if there is no effective international shipping regime that pre-screens sub-standard shipping.

International Considerations

In the wake of the terrorist attacks of September 11, 2001, a consensus emerged among experts involved in the issue that an effective solution for securing maritime trade requires creating an international maritime security regime. This regime would rely not on a single solution, such as increasing the number of container inspections, but rather on a layered approach with multiple lines of defense from the beginning to the final destination of a shipment. The first security perimeter in this "defense in depth" strategy would be at the overseas point of origin.[63] Security experts argue that an effective solution must start with preventing undesired items from entering the maritime transportation network, because if some of these items — particularly nuclear weapons or dirty bombs — reach a U.S. seaport, they could be detonated before inspectors could find them.

A related issue is whether raising international port security standards should become part of international trade agreements. Thus far, the United States' strategy has been to raise standards by working within the maritime transportation industry, such as through the IMO. However, some assert that given the strong link between maritime security and international trade, the United States could also pursue international port security standards as part of international trade agreements.

Standard vs. Site-Specific Measures

An additional issue for Congress is determining what elements of port security might be best addressed through across-the-board requirements that establish common standards and practices to be applied at all seaports, versus those elements of port security that might be best addressed through a tailored, bottom-up approach that employs measures that are designed to fit the specific circumstances and meet specific needs of each seaport.

Some observers, while acknowledging the need for site-specific measures, argue that a certain amount of uniform measures are necessary to help ensure that no seaport remains excessively vulnerable to terrorist attack. Other observers argue that while standardized measures make sense up to a point, the effort to implement such measures must not come at the expense of efforts to devise and implement site-specific security measures that respond to the unique characteristics of each port. Compared to commercial airports, seaports are generally more diverse in terms of their physical infrastructure and operations. As a result of this diversity in characteristics, each ship and port facility presents different risks and vulnerabilities.

Port authorities are also very concerned with finding the right balance between standard and port specific security regulations. Ports seek a level of uniformity in security requirements because they are concerned that their customers will move their

---

[63] A leading advocate for point of origin security is Stephen Flynn; see "Beyond Border Control," *Foreign Affairs*, Nov./Dec. 2000.

business to competing ports where their goods may be cleared more quickly. At the same time, ports do not want to be held to inflexible federal standards. They are concerned that setting security benchmarks may waste time and resources if those benchmarks are not applicable at their port given their particular commodity mix or other unique circumstances.

Security Cards. In addition to improving the security infrastructure of U.S. ports, there is also the issue of ensuring the trustworthiness of the people who work in them. Issuing credentials for port workers illustrates the challenge of implementing standard security measures. One of the difficult questions is what should disqualify someone from holding a job in a port area. MTSA (Section 70105) requires the Secretary of Homeland Security to develop a transportation security card for port workers that would be used to limit access to secure areas in a port.[64] Among the items that would disqualify a port worker from obtaining a card would be a felony conviction within the last seven years that the Secretary believes could cause the individual to be a terrorism risk.[65] The USA PATRIOT Act (P.L. 107-273) passed in October 2001, requires background checks for truckers carrying hazardous materials. The TSA is developing a "Transportation Worker Identification Credential" (TWIC) Program that will use biometric cards issued to all transportation workers to limit access to secure areas in the nationwide transportation network.

Issuing transportation ID cards is an example of an across-the-board requirement. However, the difficulty of implementing such measures at specific ports is illustrated below:[66]

> ...Tampa offers a good example. Some of the port's major employers consist of ship repair companies that hire hundreds of workers for short-term projects as the need arises. Historically, according to port authority officials, these workers have included persons with criminal records. However, new state requirements for background checks, as part of issuing credentials, could deny such persons needed access to restricted areas of the port. From a security standpoint, excluding such persons may be advisable; but from an economic standpoint, a company may have difficulty filling jobs if it cannot include such persons in the labor pool.

Roles and Responsibilities

A major concern for U.S. policymakers is assigning roles and responsibilities for maritime security among federal agencies, among federal, state, and local agencies, and between government agencies and private industry. Clear roles and

---

[64] For a status report on progress towards development of this card, see GAO Report GAO-05-106, *Port Security[:] Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* December 2004.

[65] Preexisting regulations regarding the issuing of Coast Guard port security cards are contained at 33 C.F.R. Part 125 — Identification Credentials for Persons Requiring Access to Waterfront Facilities or Vessels.

[66] GAO, *Port Security, Nation Faces Formidable Challenges in Making New Initiatives Successful,* GAO-02-993T, p. 13.

responsibilities are needed to prevent overlap, duplication of effort, and conflicting regulations. It is critical that the maritime trade community perceives that federal agencies are working in concert, otherwise the DHS's goal of a close partnership with industry in fighting terrorism may be frustrated.

Intelligence Sharing. The difficulty of detecting terrorist activity once it has entered the maritime system may point to the value of intelligence. Most acknowledge that there is just too much cargo, coming from all corners of the globe, to scrutinize each shipment thoroughly. Uncovering terrorist activity is likely to require "actionable" or precise intelligence identifying exactly which shipment to intercept. One of TSA's critical missions is to ensure that threat information gathered by other federal agencies, such as the FBI or CIA, is shared with appropriate transportation officials. The GAO reports that "in surface transportation, timely information-sharing has been hampered by the lack of standard protocols to exchange information among federal, state, and local government agencies and private entities."[67] One barrier to more effective intelligence sharing with local port authorities may be that state and local government officials do not have the required security clearances.

Private Industry's Role. A broad policy question for Congress is how much of a role the private sector should have in enhancing maritime security. Many observers believe that businesses will worry more about near term profits than the remote possibility that their property will be attacked.[68] At the same time, most experts acknowledge that there are just too many cargo movements for the government to monitor on its own. Security experts believe that tightening control over maritime commerce requires that security be "embedded" into everyday business processes. CBP's C-TPAT program is intended to enlist the effort of the many companies involved in international container shipments. In its oversight responsibilities, Congress may evaluate the effectiveness of this program, particularly in ensuring the due diligence of maritime traders over the long term. Congress may consider how best to ensure sustained follow through on the part of C-TPAT participants. A "trust but verify" approach utilizing regular CBP security audits may be one strategy policymakers consider.

---

[67] GAO, *Transportation Security, Post-September 11th Initiatives and Long-Term Challenges*, April 1, 2003, GAO-03-616T.

[68] "Gaps in Our Defenses," *Baltimore Sun*, Feb. 12, 2003.