

CRS Report for Congress

Received through the CRS Web

Maritime Security: Overview of Issues

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

Summary

In the wake of the terrorist attacks of September 11, 2001, port security has emerged as a significant part of the overall debate on U.S. homeland security. Many security experts believe ports are vulnerable to terrorist attack because of their size, easy accessibility by water and land, and the tremendous amount of cargo they handle. To raise port security standards, Congress passed the Maritime Transportation Security Act of 2002 (P.L. 107-295) in November 2002. In the 108th Congress, there is growing debate about whether current efforts to improve port security are proceeding at sufficient pace and whether the nation is devoting enough resources for this purpose. This report will be updated periodically.

Concerns for Port Security

Government leaders and security experts worry 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.¹ They are also concerned that ships in U.S. ports, particularly large commercial cargo ships or cruise ships, could be attacked by terrorists. A large-scale terrorist attack at a U.S. port, experts warn, could not only cause local death and damage, but also paralyze global maritime commerce.

Even before the terrorist attacks of September 11, 2001, government officials and security experts were concerned about the security of U.S. ports. 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 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.² To address the concerns raised in the report, Senator Hollings introduced S. 1214, the Maritime Transportation Security Act of 2001 on July 20, 2001. On November 14,

¹ For further information on this topic, see: CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress*; and CRS Report RS21293, *Terrorist Nuclear Attacks on Seaports: Threat and Response*.

² *Report of the Interagency Commission on Crime and Security in U.S. Seaports*, Fall 2000, p. 63.

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.

Features of the U.S. Maritime System

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.³ Transportation firms tend to concentrate traffic through major cargo hubs because of the high cost of their infrastructure.⁴ 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.⁵

In 2001, approximately 5,400 commercial ships made more than 60,000 U.S. port calls. Most ships calling U.S. ports are foreign owned and foreign crewed; less than 3% of U.S. overseas trade is carried on U.S.-flag vessels.⁶ The lack of transparency in ship ownership has been a longstanding concern. Shipowners can register their ships in “flag of convenience” countries which may have lax regulations and require little information from the applicants.⁷

Container ships are a growing segment of maritime commerce – and the focus of much of the attention on seaport security. While they carry only 11% of annual tonnage, they account for 66% of the total value of U.S. maritime overseas trade. 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 8x8x20 feet or 8x8x40 feet. More than 6 million cargo containers from all corners of the globe enter U.S. seaports each year. The Bureau of Customs and Border Protection (CBP) analyzes cargo manifest information for each container to decide which to target for closer inspection but only a small percentage have their contents physically inspected by CBP.

Ships are the primary mode of transportation for world trade. Ships carry more than 95% of the nation’s non-North American trade by weight and 75% by value. Waterborne cargo contributes about 7.5% to the U.S. gross domestic product.⁸ Given the importance

³ For a more detailed description of 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/>].

⁴ 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 [www.iwr.usace.army.mil/ndc/].

⁵ U.S. Congress, House of Representatives, Maritime Transportation Security Act of 2002, Conference Report, H.Rept. 107-777, p. 4.

⁶ “The Maritime Component,” *Sea Power*, August 2001.

⁷ See William Langewiesche, “Anarchy at Sea,” *Atlantic Monthly*, Sept. 2003, p.50. And, OECD, *Ownership and Control of Ships*, Maritime Transport Committee, March 2003.

⁸ Admiral Thomas H. Collins, Commandant, U.S. Coast Guard, speech before the International Maritime and Port Security Conference, Singapore, Jan. 21, 2003.

of maritime trade to the U.S. economy, disruptions to that trade can have immediate and significant economic impacts.

Recent Port Security Initiatives by Federal Authorities

Leading federal agencies involved in port security include the Coast Guard, the Bureau of Customs and Border Protection (CBP), and the Transportation Security Administration (TSA), all of which are housed in the Department of Homeland Security (DHS). 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, passengers or crew destined for the United States. By increasing their knowledge of the various parties in the marine environment, it is hoped that federal inspectors will be better able to separate the bad from the good without impeding the flow of legitimate travel and commerce.

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.⁹ 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 the 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. The Coast Guard issued final rules implementing MTSA on October 22, 2003 (see 68 Fed. Reg. 60448).

The Coast Guard refers to its efforts at improving its knowledge of the ships calling at U.S. ports as "Maritime Domain Awareness" (MDA). The Coast Guard has instituted new reporting requirements for ships entering 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 NOA is evaluated to select certain high-interest vessels for boarding by Coast Guard port security teams. Coast Guard sea marshals may also escort certain ships transiting the harbor.

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. 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 stationing U.S. inspectors at

⁹ 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 Coast Guard's and Navy's role in homeland security, see CRS Report RS21230, *Homeland Security: Navy Operations – Background and Issues for Congress*, and CRS Report RS21125, *Homeland Security: Coast Guard Operations - Background and Issues for Congress*.

selected foreign ports to pre-screen U.S.-bound containers. 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.

C-TPAT, initiated in April 2002, offers importers expedited processing of cargo if they comply with CBP guidelines for securing their 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. One of the key security controls recommended in the program is for shippers to have a “designated security officer” to supervise the container loading process as protection against the introduction of illegal material.¹⁰ If CBP certifies an applicant, they may benefit from a reduced number of cargo inspections, thus reducing the risk of shipment delay.

Transportation Security Administration. TSA was created by the Aviation and Transportation Security Act of 2001 (P.L. 107-71) which was signed into law on November 19, 2001. TSA is responsible for the security of all modes of transportation, cargo and passenger. TSA, in conjunction with CBP, is conducting a pilot project called Operation Safe Commerce (OSC).¹¹ The goal of OSC is to verify the contents of sea 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. 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.

Issues for Congress

Addressing the Threat. A major concern for Congress is assessing whether the nation is doing enough and fast enough to deter a terrorist attack in the maritime domain. 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.¹² Seaports, along with air cargo, general aviation, and mass transit, were identified in a April 2003 GAO report as the “major vulnerabilities” remaining in the nation’s transportation system.¹³ 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

¹⁰ Further details of the C-TPAT program are available at [<http://www.cbp.gov/xp/cgov/home.xml>] (viewed 12/4/03).

¹¹ Federal Register, Nov. 2, 2002, p. 70110-70112.

¹² “Safe Harbors?” *The Wall Street Journal*, April 21, 2003, p. B1. Also, Maarten van de Voort and Kevin A. O’Brien, et. al., *Seacurity*, RAND Europe, 2003.

¹³ GAO, *Transportation Security, Post September 11th Initiatives and Long-Term Challenges*, April 1, 2003, GAO-03-616T.

framework for building a maritime security regime, and that significant gaps in security still remain. In the words of one security expert,¹⁴

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.

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 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.¹⁵ Congress has provided over \$500 million through FY2004 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.¹⁶ Advocates for more spending argue that the federal grants provided to port authorities thus far is only a fraction of the amount that is needed. 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.

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 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.¹⁷ Finding the right balance between improving

¹⁴ Stephen Flynn, "On The Record," *Government Executive Magazine*, October 1, 2003.

¹⁵ See Federal Register, October 22, 2003 vol. 68, no. 204, p. 60464.

¹⁶ See CRS Report RL32061, *Border and Transportation Security: Budget for FY2003 and FY2004*.

¹⁷ 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.

cargo security to desired levels without unduly impeding the legitimate flow of commerce is a difficult issue.

Security of Ships. 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, the International Maritime Organization (IMO), a branch of the United Nations, adopted more stringent international standards for the security of vessels and ports (titled the International Ship and Port Facility Security Code, ISPS). 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. While the United States enforces its standards when the Coast Guard selects arriving ships for boarding, their burden is greater if there is no effective international shipping regime to pre-screen sub-standard shipping.

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 physically inspect 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.”¹⁸ 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.

¹⁸ GAO, *Transportation Security, Post-September 11th Initiatives and Long-Term Challenges*, April 1, 2003, GAO-03-616T.