Order Code RL33383

CRS Report for Congress

Terminal Operators and Their Role in U.S. Port and Maritime Security

Updated January 19, 2007

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

Jennifer E. Lake
Analyst in Domestic Security
Domestic Social Policy Division

Prepared for Members and
Committees of Congress

Terminal Operators and Their Role in U.S. Port and Maritime Security

Summary

The failed attempt by Dubai Ports World (DP World) to operate marine terminals at some U.S. ports raises the issue of whether foreign marine terminal operators pose a threat to U.S. homeland security. Notwithstanding the sale of U.S. terminal operations by DP World to a U.S. entity, the underlying issue remains because many U.S. marine terminals are operated by foreign-based companies and a similar transaction could occur in the future, given the global nature of the shipping industry.

Evaluating the potential security ramifications of foreign-based terminal operators requires first understanding how ports work and who is in charge of their security. Most major U.S. ports are publicly owned by a "port authority," which is a public organization associated with a city, county, regional, or state government. A port typically contains many terminals that are each designed to handle different types of cargo. Some port authorities operate all or some of their marine terminals, but most ports lease their facilities to several different terminal operating companies. All of the cargo handling that takes place on a marine terminal is performed by members of a longshoremen's union.

The Coast Guard is in charge of the security of port facilities and vessels, and Customs and Border Protection (CBP) is in charge of the security of cargo. Coast Guard regulations and CBP security guidelines require terminal operators to provide basic security infrastructure, such as fences, gates, and surveillance cameras, and follow certain security practices when handling cargo. The Transportation Security Administration (TSA) is developing a credentialing process for screening port workers. However, port security involves much more than the measures put in place within the immediate vicinity of a U.S. port complex. Not finding a terrorist-placed weapon until after it reaches a U.S. port could be too late to prevent a potentially catastrophic event. Thus, securing the cargo and ships in transit to U.S. ports is critical and consequently the bulk of federal security activity takes place before cargo is unloaded at U.S. ports. Key layers of security are CBP's scrutiny of U.S.-bound cargo at the *overseas port of loading* and the Coast Guard's scrutiny of ships *before* they enter U.S. harbors.

The necessity of pushing the border out to counter the terrorist threat requires the cooperation of shippers, carriers, ports, and border agencies in the country of origin to take security precautions with U.S.-bound cargo. Global terminal operators like DP World may handle U.S. cargo at the overseas loading port, even if they do not handle it at a U.S. port. Thus, a key issue for policymakers is deciding under what conditions the United States should trust foreign cargo-handling entities and whether they should be treated as partners in securing U.S. supply lines. The DP World controversy refueled debate about whether the nation is doing enough, with sufficient urgency, to secure U.S. ports. In its oversight role, Congress is assessing the effectiveness of Coast Guard and CBP maritime security initiatives and faces pressing questions about the overall security of ports and maritime commerce.

Contents

Terminal Operators and Their Role in U.S. Port and Maritime Security

The failed attempt by Dubai Ports World (DP World) to operate marine terminals at some U.S. ports raises the issue of whether foreign marine terminal operators pose a threat to U.S. homeland security. DP World is a terminal operating company that operates as a commercial entity, but is owned by the Government of Dubai in the United Arab Emirates.[1] DP World recently purchased a competitor, the British-owned Peninsular & Oriental Steam Navigation Company (P&O). P&O leases marine terminals around the world, including at five U.S. ports – New York and New Jersey, Philadelphia, Baltimore, Miami, and New Orleans, and is involved in other cargo handling operations at other East and Gulf Coast ports, as well as a cruise terminal in New York City. As part of DP World's purchase of P&O, DP World would have acquired P&O's terminal leases or concessions at these U.S. ports.[2] However, as a result of Congressional opposition, DP World announced on March 9, 2006 that it will sell its stake in the U.S. portion of P&O's operations to a U.S. entity.[3]

Notwithstanding the sale of U.S. terminal operations by DP World to a U.S. entity, the underlying issues remain: Is the ownership of a terminal operating company relevant to the security of a U.S. port? Does foreign takeover of terminal operating leases potentially pose a threat to U.S. security? Should companies owned by foreign governments be precluded from operating U.S. port terminals? These policy questions remain an issue because (1) many U.S. marine terminals are operated by foreign-based companies, and (2) given the global nature of the shipping business, similar transactions may occur in the future.

The purpose of this report is to provide information relevant in answering these questions. It begins by explaining how ports work and what marine terminal operators do. It then reviews the extent of foreign involvement that already exists in U.S. ports. The next section describes the responsibility of terminal operators in providing security at U.S. ports and how their role fits in with the larger task of

---

[1] For further information on the United Arab Emirates, see CRS Report RS21852, *The United Arab Emirates (UAE): Issues for U.S. Policy*, by Kenneth Katzman.

[2] The Committee on Foreign Investment in the United States (CFIUS) reviewed and approved this transaction. For further information on CFIUS, see CRS Report RL33312, *The Exon-Florio National Security Test for Foreign Investment,* by James K. Jackson.

[3] On December 11, 2006, DP World announced that it had entered into an agreement with a wholly owned subsidiary of AIG Global Investment Group to sell its stake in the U.S. portion of P&O's operations. The text of this announcement is available at [http://www.dpworld.com].

securing the entire maritime supply chain. The report concludes by examining port security issues for Congress.

Port Administration and Operation

The debate over the DP World transaction often confused the terms "port," "port authority," and "terminal." Most major U.S. ports are publicly owned by a "port authority," which is a public or quasi-public organization associated with a city, county, regional, or state government. A port authority is responsible for the overall administration of the property, terminals, and other facilities on the port complex. A marine terminal is an assigned area with equipment for loading and unloading ships, and space for staging cargo until it is loaded on the ship or transferred to overland modes of transport. Some port authorities operate all or some of their marine terminals themselves, but most ports are "landlord" ports because they lease their facilities to terminal operating companies (the tenants). These leases are typically long-term – in the range of 10 to 30 years. Either the port authority or the terminal operator will supply the cranes and other cargo handling equipment. It depends on the lease agreement between the port authority and each terminal operator.

As one port authority suggests, one can think of a public port like a shopping mall.[4] The port authority owns the entire mall property while the stores are leased to individual retail companies. A large port could contain 15 to 20 marine terminals of various types. Some of the terminals could handle containers (which are truck-trailers without the wheels), others may handle dry bulk cargo (such as coal, grain, or sugar), liquid bulk cargo (such as petroleum or chemicals), breakbulk cargo (such as steel coils, pipes, or large machinery), or automobiles and trucks. A typical container terminal may be 100 to 300 acres in size, while the entire port complex of a major port may be 2,000 to over 3,000 acres in size.

While the above model applies to the marine terminals involved in the DP World transaction, it does not apply to all marine terminals. Public port authorities only own approximately one-third of the deep-draft marine terminal facilities in the United States.[5] Many of the privately owned marine terminals are associated with the oil, gas, and chemical industries. In these cases, the waterside terminal may be a component of a larger industrial complex on land. For instance, at the Port of Houston, the Port of Houston Authority only owns or leases 12 marine terminals while there are 138 private terminals that are owned by either U.S.-based, foreign-based, or multi-national corporations that handle approximately 85% of the cargo that moves through the Port of Houston.[6]

---

[4] An analogy used by the Port of Tacoma, "Questions and Answers: Port Terminal Ownership, Operations, and Security," February 24, 2006, Press Release.

[5] U.S. Maritime Administration, *U.S. Public Port Development Expenditure Report*, November 2005, p. 1.

[6] Port of Houston Authority, Fact Sheet, available at [http://www.portofhouston.com].

Terminal operators (a.k.a. stevedores) contract with longshoremen unions to provide cargo handling services on the docks.[7] Longshoremen are hired by and report directly to a union hiring hall. Terminal operators also employ a management team who are hired by and report directly to the terminal operating company. Longshoremen, called "dockworkers," operate cranes that physically move the cargo from ship to dock and vice versa. Longshoremen, called "checkers," perform clerk functions in an office in or near the port. At a container terminal, the checkers are responsible for directing the container traffic within the terminal area – they tell the dockworkers where containers need to be moved. The ocean carrier provides a stowage plan which tells the terminal operator where the containers need to be loaded on the ship. In the case of inbound shipments, the terminal operator separates those containers to be picked up by truck from those that will move by rail (if there is an "on-dock" railroad at the terminal). Longshoremen also staff the gates where trucks enter to pick-up and drop-off containers.

Longshoremen do not know the contents of containers except for containers carrying hazardous material, which require special handling and storage requirements. The terminal operator is not concerned with the origin and final destination of the shipment.[8] The only cargo information relevant to the terminal operator in performing its function is the weight of the container (for ship loading purposes), whether or not it has been released by Customs (for imported cargo), the bill of lading number (or booking number for export cargo), seal number, and container number.

An Industry Driven by Globalization

While DP World would have been the first Middle Eastern based company to operate container terminals in U.S. ports, most container terminals are operated by other foreign-based companies. A survey by the U.S. Maritime Administration found that at the seventeen largest U.S. container ports, 45 terminals (66%) were operated by a foreign based company, 5 terminals (7%) were operated by a joint venture between a domestic and foreign based company, and 18 terminals (26%) were operated by a purely domestic terminal operating company. The survey found that several of the ports have no U.S.-based container terminal operators: Baltimore, Jacksonville, New Orleans, Houston, Los Angeles, and Tacoma. At the combined Ports of Los Angeles and Long Beach, the largest container port complex in the United States, only three of the fifteen container terminals are operated by U.S.-based companies. At the Port of New York and New Jersey, the second largest container port, only two of the six container terminals are operated by U.S.-based companies. At the Port of Norfolk and the Port of Savannah, the port authority operates the

---

[7] The longshoremen unions negotiate their contracts with a trade association that represents terminal operators.

[8] Testimony of Robert Scavone, P&O Ports North America, House Committee on Transportation and Infrastructure, Subcommittee on Coast Guard and Maritime Transportation, hearing on Implementation of Port Security Programs, March 9, 2006.

terminals rather than leasing them to private terminal operators.[9] The Port of Portland (Oregon) leases its container terminal to a U.S. based operator. Most of the foreign terminal operators are based in Hong Kong, Japan, South Korea, Taiwan, Singapore, China, the United Kingdom, and Denmark. A handful of terminal operators are partially owned by the governments of Singapore, Taiwan, and China.

Most U.S. container terminals are managed by foreign companies because almost all of the container shipping lines are owned by foreign companies. Typically, a foreign container shipping line creates a U.S. subsidiary or a U.S. affiliate to operate the terminals at its busiest U.S. ports to better ensure service quality and control costs. Two large U.S.-based container lines and their terminal operations were sold to foreign interests in the late 1990s. In 1997, American President Lines was sold to Neptune Orient Lines, which is partially owned by the government of Singapore. In 1999, Sea-Land Service, the U.S. company that pioneered container shipping in the late 1950s, was sold to Maersk Lines, a Danish carrier. The president of the World Shipping Council (WSC) who is also a former executive of Sea-Land believes that U.S. investors have avoided the container shipping industry because of its high capital investment requirements, "boom and bust" cycles, intense competition, and because foreign tax laws are more favorable to shipping.[10]

While many terminal operators are affiliated with a steamship line, independent terminal operating companies also exist. DP World and P&O are two of several global terminal operating companies. Other global stevedores are Hutchison Port Holdings, based in Hong Kong; PSA, based in Singapore; and SSA Marine, based in Seattle. One estimate is that the four largest global terminal operators handle about 80% of the containers being shipped worldwide.[11] Some U.S. independent terminal operators only operate in the United States, such as Maher Terminals and American Stevedores in New York, and Transbay and Marine Terminals Corporation in Oakland.

Foreign involvement in U.S. port terminal operations is an extension of an industry driven by globalization. The largest container shipping lines have extended their services around the globe because their biggest customers, such as big box retailers and auto, electronics, and clothing manufactures, have extended their supply lines and distribution networks around the globe. In turn, global independent terminal operators, such as DP World or P&O, seek to follow their customers, the shipping lines. The shipping business is capable of scanning the globe for low-cost inputs. For instance, it is not improbable that a ship calling at a U.S. port could have been built in South Korea, registered in Panama, owned by a Greek company, operated by a Japanese ocean carrier, captained by a German, and crewed by Filipinos.

---

[9] Except that a foreign company has a 50% stake in the operations of one of the terminals at the Port of Norfolk.

[10] Testimony of Christopher Koch, President and CEO of the World Shipping Council, House Homeland Security Committee, Hearing on SAFE Port Act, April 4, 2006.

[11] Testimony of Gary Gilbert, Senior Vice President, Hutchison Port Holdings, Senate Committee on Homeland Security and Governmental Affairs, Subcommittee on Investigations, Hearing on Securing the Global Supply Chain, March 30, 2006.

Security Requirements of Terminal Operators

Terminal operators are responsible for maintaining security on the property they rent from the port authority. Coast Guard regulations and Customs and Border Protection (CBP) security guidelines require terminal operators to provide basic security infrastructure and follow certain security practices when handling cargo. These requirements are reviewed in some detail below because they indicate the specific responsibilities of a terminal operator in providing security at a port.

Coast Guard Requirements

The Coast Guard is in charge of the security of port facilities and vessels, under the terms of the Ports and Waterways Safety Act of 1972 (P.L. 92-340) and the Maritime Transportation Security Act of 2002 (MTSA[12], P.L. 107-295).[13]

Facility Security Plan. Each terminal operator in a port area is required to conduct a security assessment of their facility as well as write a security plan and submit it to the Coast Guard for review and approval.[14] The Coast Guard does not mandate specific security equipment or procedures that the terminal operators must adopt but rather calls for "performance-based" criteria to be used to ensure the security of the facility. The security plan provides some leeway for the terminal operators to tailor their security measures to their particular type of cargo terminal.

In the facility security plan, the terminal owner or operator must specify how it will address the security vulnerabilities identified in its security assessment. For instance, it must restrict access to its facility with fences and a system to identify unauthorized personnel. The operator must specify how it will monitor activity at the facility through the use of some combination of security guards, water-borne patrols, alarm systems, surveillance equipment, and lighting. In the case of container facilities, the operator must specify how it will check container seals and verify that arriving trucks have legitimate business at the facility. The facility operator must conduct periodic security drills and exercises. It is required to designate a Facility Security Officer (FSO) who is responsible for ensuring that the facility is in compliance with Coast Guard regulations and serves as the point of contact for notifying security threat level changes. The FSO is also required to keep records for two years and make them available to the Coast Guard regarding security training sessions, drills and exercises, security incidents and breaches, changes in security threat levels, maintenance of security equipment, and other records regarding security procedures at the terminal.

The Coast Guard inspects terminals for compliance with security requirements. July 1, 2004 was the deadline for port facilities to begin operating under their security

---

[12] MTSA regulations are codified at 33 CFR 101 et. seq.

[13] The Coast Guard is also charged with a number of non-homeland security missions: marine safety, marine environmental protection, fisheries enforcement, aids to navigation, and others.

[14] See 33 CFR Part 105 for a complete listing of port facility security requirements.

plans. Between then and January 1, 2005, the Coast Guard conducted initial on-site inspections at approximately 3,150 port facilities in more than 300 U.S. ports to check on compliance with the security plans. The Coast Guard plans to conduct annual compliance inspections at port facilities but the Coast Guard Captain of the Port, which is the lead federal official in charge of a port area, can also verify continued compliance at the facilities in his or her area at any time. To ensure that inspections reflect the normal course of business at a terminal, the Coast Guard has indicated that it is using unscheduled or unannounced spot checks to check on compliance.[15] The Coast Guard reports that since July 2004, it has required corrective action on more than 700 violations of the MTSA security regulations and that of those 700 plus violations, 44 resulted in major control actions, such as closure of the terminal until corrective action was taken.[16]

Similar to terminal operators, vessel owners must also submit for Coast Guard approval a security assessment and security plan for their ships. Because of the close interface between vessels and facilities (when the vessel is in port), vessel and facility owners are required to coordinate their security measures and procedures and submit evidence of this coordination in a document called a "Declaration of Security." Facility and vessel owners are required to update and resubmit their security plans to the Coast Guard every five years or whenever a substantial change is made to their facility or vessel.

CBP's Requirements

CBP is in charge of cargo security. When CBP inspects cargo shipments arriving from overseas, the terminal operator's role is to set those shipments aside as CBP directs. CBP is the primary federal agency tasked with ensuring the security of the nation's borders.[17] CBP's port security mission is to prevent terrorists and instruments of terror from entering the United States. Like the Coast Guard, CBP faces the difficult challenge of achieving a sufficient level of security while not jeopardizing the efficient flow of commercial goods at the nation's ports of entry (POE). Generally, every shipment, whether it arrives via maritime, truck, rail, or air cargo container, must be released by CBP before it may enter the commerce of the United States. CBP is not only responsible for ensuring the security of the containers (in terms of preventing their subversion by terrorists and other criminals), but is also responsible for ensuring that the cargo does not violate any commercial laws of the United States.

---

[15] GAO, *Coast Guard: Observations on Agency Priorities in FY2006 Budget Request*, March 17, 2005, GAO-05-364T, p. 10.

[16] Testimony of Rear Admiral Thomas Gilmour, U.S. Coast Guard, House Armed Services Committee hearing, *National Security Implications of Dubai Ports World's Takeover of U.S. Ports*, March 2, 2006.

[17] CBP was created in the reorganization that followed the creation of the Department of Homeland Security (DHS) with the passage of the Homeland Security Act of 2002 (P.L. 107-296), and is comprised of the inspection functions of the legacy US Customs Service, Immigration and Naturalization Service, the U.S. Border Patrol, and a portion of the inspectors of the Animal and Plant Health Inspection Service. CBP is also home to CBP Air and Marine.

Customs-Trade Partnership Against Terrorism. The Customs-Trade Partnership Against Terrorism (C-TPAT) was initiated in April 2002 as a voluntary program offering importers expedited processing of cargo and other benefits if they comply with CBP requirements for securing their entire supply chain. Currently, C-TPAT is open to importers, carriers, freight forwarders, customs brokers, U.S. port authorities, terminal operators, and Mexican and other CBP-invited foreign manufacturers. In order to participate in the C-TPAT, applicants must sign an agreement that commits them to assessing the security of their supply chains, submit a security questionnaire to CBP, implement a security program in accordance with C-TPAT guidelines, and extend their security program to other companies involved in their supply chain.

Once the applicant company has conducted the security self-assessment and submitted the security profile, CBP reviews the security profile to develop an understanding of the company's security practices. CBP also reviews information regarding the company's trade compliance history and any past criminal investigations. Based upon the results of these reviews, CBP will work with the applicant to address any security concerns discovered during the review, or will certify the applicant as a C-TPAT certified member. CBP also conducts what is called a 'validation' of a C-TPAT certified members' security arrangements. The validation process is an on-site review of the supply chain security measures outlined by the C-TPAT participant in the security profile it submitted to CBP. CBP has created Supply Chain Security Specialists (SCSS), who conduct the validation. During the validation process, the SCSS will meet with company representatives and potentially visit selected domestic and foreign sites in the C-TPAT participant's supply chain.[18]

C-TPAT security guidelines differ depending on the type of business the applicant is engaged in. For instance, importers have a different set of security guidelines than carriers, or port or terminal operators; and C-TPAT guidelines recognize that terminals, for example, vary according to the type of cargo they handle. As with other C-TPAT participants, U.S. Marine or Port Terminal Operators (MPTO) must conduct a comprehensive assessment of their international supply chain (conveyances, foreign facilities, domestic warehouses, etc.) and work with their business partners to ensure that the appropriate security measures are adhered to throughout their supply chain. The security guidelines that MPTO must commit to implementing and maintaining throughout their supply chains in order to become a member of C-TPAT include the following categories: conveyance security (to prevent unauthorized access or tampering); business partner requirements and security procedures (to ensure that partners commit to C-TPAT guidelines); container security (procedures for ensuring proper sealing and container integrity, along with procedures to report any problems to CBP); physical access controls (identification badges, visitor and vendor controls, mail screening etc.); procedural security; personnel security (background checks and investigations, etc.); physical security

---

[18] CBP, "C-TPAT Validation Fact Sheet," accessed at [http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/validation_fact_sheet.xml].

(fences, gates, cameras, alarms systems, etc.); and information technology security.[19] As the above discussion indicates, C-TPAT requirements for Port Authorities and Terminal Operators are similar to the Coast Guard's security requirements.

Security Infrastructure

Whether the terminal operator or the port authority is responsible for providing basic security infrastructure, such as perimeter fencing, security gates, lighting, monitoring equipment, or alarm systems, is likely to be addressed in the terms and conditions of the lease agreement between the port authority and the terminal operator. The geography of a port complex is one factor that could determine infrastructure security arrangements. For instance, if there are a group of terminals that abut one another, then the port authority may be the party that provides perimeter fencing and a perimeter security gate for access to all the grouped terminals. On the other hand, if a particular terminal is isolated from other terminals in a port complex, then the terminal operator may be responsible for providing security infrastructure. The federal government has provided funding directly to ports for security infrastructure. Since September 11, 2001, the federal government has provided about $876 million in six rounds of grants to port authorities and individual terminal operators for security infrastructure.[20]

Security Personnel

Either the port authority or the terminal operator hires security guards. Within the grounds of a terminal, there may be security guard and "port watchmen" positions defined in the contract between the longshoremen's union and the terminal operator. A few of the largest port authorities have their own police force. The port authority police force could include both waterside and landside patrols, and police assigned to port gates. Other port authorities rely on the police force of the government with which they are associated, such as city, county, or state police.

Screening Port Workers

A key issue in port security is the trustworthiness of the people who work in them. As per MTSA (46 USC 70105), DHS is responsible for determining whether a port worker poses a potential terrorism security risk. The Coast Guard is assisting the Transportation Security Administration (TSA) in developing a worker identification card (Transportation Worker Identification Credential, TWIC) that will be used to limit access to secure areas of a port or vessel. MTSA requires that the card use biometric technology and that the card be issued to only those port workers

---

[19] See, CBP, "Online Application for U.S. Marine Port Authority/Terminal Operators," [http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/onlinectpat_app_process/marine/app_marine_port_auth_operators.xml] for a more complete discussion of these guidelines.

[20] Association of American Port Authorities, [http://www.aapa-ports.org].

who are not deemed a terrorism security risk as determined by the Secretary of DHS.[21]

TSA's initial deadline for issuing TWIC cards was August 2004. The GAO investigated why TSA missed its initial deadline and found that delays were due to difficulty in obtaining DHS approval to proceed with the prototype phase, extra time needed to collect data for a cost-benefit analysis, and additional work required to assess card technologies.[22] The agencies tested a prototype worker card at various ports in 2005 and implementation of the card is to begin in 2007. A contentious issue, among several, is deciding what criminal offenses might disqualify a worker from obtaining a card.

Most port authorities are awaiting the deployment of the TWIC card to provide an ID system for port workers. However, a couple of port authorities have an ID card system already in place. The Port Authority of New York and New Jersey has had an ID system for dockworkers since 1953. The Waterfront Commission of New York Harbor performs background checks on all longshoremen at the port, who must be registered and licensed. The Commission was created in 1953 to fight corruption at the port. The Port of Miami introduced an ID system a few years ago.[23] Three port authorities in Florida have begun implementing a state-wide ID system to fulfill requirements of a Florida state law on port security.[24] The Florida law requires a fingerprint-based criminal history check of port workers.

As long and difficult as it has been to develop a background check and ID system for U.S. port workers, this effort concerns only one node in the maritime transportation system. The United States has no jurisdiction over transportation workers in overseas ports, as well as the truck drivers, rail workers, and others who directly handle the cargo on its way to the overseas port. One of the criteria for C-TPAT participants is to conduct background checks on their employees. However, it is not known how or if CBP validates these checks. While background checks can provide some level of assurance as to the trustworthiness of a worker, experience has shown that individuals, who have undergone much greater scrutiny, such as high level security clearances, have occasionally proven untrustworthy.

---

[21] MTSA (116 STAT. 2073) provides some guidance as to determining terrorism risk and requires an appeals process for those found ineligible for a card.

[22] GAO Report GAO-05-106, *Port Security: Better Planning Needed to Develop and Operate Maritime Worker Identification Card Program,* December 2004. TWIC delays were also the subject of a congressional hearing, House Transportation and Infrastructure Committee, Subcommittee on Coast Guard and Maritime Transportation, *Field Hearing on National Strategy for Maritime Security,* January 24, 2006.

[23] "Where's Your ID?" *Journal of Commerce,* November 12, 2001, p.44.

[24] "Not Waiting for TSA," *Journal of Commerce,* February 20, 2006, p.16.

Security Extends Beyond the Port

Port security involves much more than the measures put in place within the immediate vicinity of a U.S. port complex. Securing the cargo and ships in transit to U.S. ports is arguably more critical and consequently the bulk of security activity takes place before cargo is unloaded at U.S. ports. While U.S. ports are an acceptable place to interdict illegal drugs and enforce trade laws, not finding a terrorist weapon until after it reaches a U.S. port could be too late to prevent a potentially catastrophic event. In response to this reality, the Coast Guard and CBP have adopted a strategy of "pushing the borders out" with a layered system of security measures. Key elements in this layered strategy are CBP's scrutiny of U.S. bound cargo at the *overseas port of loading* and the Coast Guard's scrutiny of ships *before* they enter U.S. harbors. Thus, with respect to anti-terrorism measures, U.S. ports are viewed as the last line of defense rather than the first.

Overseas Activity

Coast Guard. Recognizing the international nature of the shipping industry, the Coast Guard has sought to raise global standards for maritime security. Through the International Maritime Organization (IMO), a United Nations body that establishes shipping standards, the Coast Guard assisted in the development of a new international code for maritime security: the International Ship and Port Facility Security Code (ISPS), which went into effect on July 1, 2004. The ISPS contains security-related requirements for Governments, port authorities, and ship owners. The host government is responsible for enforcing the code. The ISPS largely parallels MTSA with respect to the security requirements of ports and ships. The Coast Guard also actively assesses the security of foreign ports that trade with the United States. The Coast Guard is visiting all of the 140 countries that trade with the United States to assess the effectiveness of anti-terrorism measures at their ports.

Vessel Screening. To counter the terrorist threat in part, the Coast Guard has sought to improve the quality and advance the timing of information submitted to them by vessels so that they can better evaluate the terrorism risk posed by ships, crews, and cargo bound for U.S. ports. After September 11, 2001, the Coast Guard instituted new reporting requirements for ships entering or leaving U.S. harbors. The former 24-hour advance Notice of Arrival (NOA) was extended to a 96-hour NOA. The NOA includes detailed information on the crew, cargo, and the vessel itself. The Coast Guard evaluates this information and other intelligence to determine what action it may take, if any, regarding the vessel. It could board and inspect the ship in the open ocean, at an anchorage near shore, at the dock, and it may escort the ship into (and out of) the port to enforce a security zone around the ship.

The Coast Guard is also deploying a vessel tracking system (the Automatic Identification System that has a range of 20-30 miles) to monitor ship traffic in U.S. harbors. This capability currently exists at 12 U.S. ports and the agency plans to extend this capability nationwide. The Coast Guard is also pursuing a long-range vessel tracking system that will have a range of about 2,000 nautical miles.

CBP. The Container Security Initiative (CSI), one of a series of initiatives aimed at improving the security of cargo destined for the United States, was initiated by the U.S. Customs Service (now CBP) in January of 2002 to prevent terrorists from exploiting containers entering into the United States. CSI is based on four core elements: (1) identifying high-risk containers; (2) pre-screening high-risk containers at the earliest possible point in the supply chain; (3) using technology to pre-screen high risk containers quickly; and (4) developing and using smart and secure containers. Under the CSI program, CBP officers are sent to participating ports where they collaborate with host country customs officers to identify and pre-screen high-risk containers using non-intrusive inspection technology before the containers are loaded on U.S.-bound ships. CSI ports provide CBP an opportunity, in cooperation with host country officials, to screen and potentially inspect cargo containers before they arrive at U.S. seaports.

CBP continues to expand CSI to additional foreign ports. By the end of 2007, CBP hopes to expand CSI to 58 ports, covering approximately 85% of the volume of maritime containers shipped to the United States. As of September 2006, CSI was operational at 50 foreign ports, covering approximately 82% of the volume of maritime containers destined for the United States.[25] The port of Dubai, United Arab Emirates, became the 35th operational CSI port on March 26, 2005.[26]

Cargo Screening. CBP's cargo inspections are dependent on receiving accurate information in a timely manner in order to execute risk assessment and targeting procedures before shipments arrive at U.S. Ports of Entry. To give inspectors adequate information and time to perform a risk assessment on arriving cargo shipments, the legacy Customs Service published a rule (known as the 24-hour rule)[27] requiring the submission of certain cargo manifest information to Customs 24 hours in advance of the vessel cargo being laden at the foreign port. The Trade Act of 2002 (P.L. 107-210), as amended, required CBP to develop rules requiring the mandatory electronic submission of cargo manifest data for all modes of entry.[28] The final rule maintained the 24-hour rule, which applies to all U.S.-bound vessel cargo.[29] The 24-hour rule applies to all U.S.-bound vessel cargo, regardless of whether or not the cargo passes through a CSI port. CBP is also exploring the acquisition of

---

[25] CBP, "Container Security Initiative Reaches Gold: Fifty Seaports Now Targeting and Pre-screening Cargo Destined for U.S." Press Release, Sept. 29, 2006.

[26] CBP, "Port of Dubai to Implement the Container Security Initiative and Begin Targeting and Pre-Screening Cargo Destined for the US," accessed at [http://www.cbp.gov/xp/cgov/newsroom/press_releases/archives/2005_press_releases/0032005/03282005.xml].

[27] U.S. Department of the Treasury, "Presentation of Vessel Cargo Declaration to Customs Before Cargo Is Laden Aboard Vessel at Foreign Port for Transport to the United States," *Federal Register*, vol. 67, no. 211, Oct. 31, 2002, pp. 66318-66333.

[28] The Trade Act of 2002 (P.L. 107-210), as amended by the Maritime Transportation Security Act of 2002 (P.L. 107-295).

[29] Department of Homeland Security, Bureau of Customs and Border Protection, "Required Advance Presentation of Cargo Information; Final Rule," *Federal Register*, vol. 68, no. 234, Dec. 5, 2003, pp. 68140-68177.

additional data that would provide CBP access to data covering the entire movement of a container: from point of packing to final destination. CBP has established a program called the Advance Trade Data Initiative (ATDI) as the prototype for the acquisition of this data.

CBP uses the Automated Targeting System (ATS) in order to identify high-risk containers requiring additional inspection. ATS uses electronically filed entry information to automatically flag high-risk shipments. ATS standardizes manifest, bill of lading, entry, and entry summary data and creates integrated records called "shipments." These shipments are then evaluated and scored by ATS using weighted rules derived from the targeting methods of experienced personnel. The higher the score, the more attention the shipment requires, and the greater the chance it will be targeted for additional enforcement actions (non-intrusive scans or physical inspection). When CBP asserts that it screens 100% of U.S.-bound cargo, it is referring to the use of the ATS system to identify high-risk containers.

Issues for Congress

The port security debate surrounding the DP World purchase of P&O has raised a number of issues for Congress. Among them are the degree to which ownership is relevant to security and what potential threats to security may stem from such ownership; the federal presence on port grounds that is necessary to insure the security of a port; and the identification and mitigation of vulnerabilities in the maritime supply chain.

Terminal Ownership and Security

At issue for policymakers is how to ensure and verify compliance with agreed-upon security standards in an environment in which terminal ownership is subject to change and frequently is foreign-based. DHS seeks a security regime which requires terminal operating companies to comply with federal security measures regardless of ownership. The Coast Guard checks for compliance with physical security requirements at the terminal. CBP, through its C-TPAT program, requires terminal operators to adhere to similar security measures. CBP is also in charge of deciding which cargo to physically inspect, with the terminal operator's role merely to set that cargo aside as CBP directs. TSA will be in charge of screening terminal workers when the TWIC card is implemented. One could argue that these measures apply equally to all terminal operators and that therefore the ownership of the terminal operating company is irrelevant to the security of a port. However, the credibility of these federal security requirements also depends on how much of an actual presence port businesses perceive federal authorities have in the port. In exercising its oversight role, Congress is likely to consider whether the Coast Guard and CBP have enough inspectors to verify compliance with agreed upon security measures.

Foreign Terminal Operators and Owners. If one believes that stevedore ownership is relevant to security, then a subsequent question is whether foreign ownership poses more of a security risk than domestic ownership. In evaluating whether foreign terminal operators should be excluded from U.S. ports, more

information as to how many U.S. marine facilities are actually operated or owned by foreign-based companies would be useful. As indicated above, most container terminals in the United States are operated by foreign companies but container terminals account for only one type of marine facility. It is probable that in some cases, other types of marine terminals are not only operated but also owned by foreign interests. While the Maritime Administration has compiled information on the ownership of container terminals at the largest U.S. container ports, similar information regarding other types of marine terminals is not readily available.

It is important to pinpoint exactly what advantage a terrorist group would have if it had some kind of connection with a terminal operator. Foreign terminal operators would gain intimate knowledge of the day-to-day security procedures at the U.S. terminals they operate and theoretically could pass this knowledge on to a terrorist group. However, U.S.-based terminal operators would have the same knowledge and a terrorist group could infiltrate them also. Because foreign terminal operators hire mostly Americans to work in their terminals, they may pose no more security risk than a U.S.-based company. One could view foreign companies like DP World as mostly the financiers behind the terminal operation with little or no involvement in the day-to-day running of the terminals.

Defining the potential threat posed by foreign terminal operators is important because there are also drawbacks to banning them from U.S. ports. Cargo security policy is about striking an appropriate balance between security and commerce. It also involves balancing security and capital investment. Port facilities depend on large capital investments. The piers, wharfs, cranes, and elevators needed to load and unload ships; the storage yards, warehouses, or tank farms needed to store cargo; the dredging of shipping channels and berths; and landside connections to interstate highways and transcontinental railroads are all expensive infrastructure. Thus, the issue of foreign terminal operators involves guaranteeing security while remaining attractive to sources of capital.

A Border-centric or Systems Approach to Security

Because it could be too late if a terrorist weapon is discovered after it arrives at a U.S. port, the security of U.S. ports necessarily relies on the cooperation of shippers, carriers, ports, terminal operators, and border agencies in the country of origin to begin the screening process. Key policy questions are: Should the United States trust these foreign entities? Should they be treated as partners and allies in securing maritime commerce? Because there are two ends to America's supply line, the answer to both may be a qualified "yes." For instance, although DP World will not be handling any U.S. cargo in U.S. ports, it will be handling U.S. cargo at ports of origin in China, Hong Kong, Europe, Southeast Asia, the Middle East, and elsewhere.[30]

---

[30] In fact, DP World is a terminal operator at three of the six overseas ports that DHS has chosen to participate in a pilot program to test the feasibility of 100% scanning of containers. See "DP World to Help Test SFI," *Traffic World*, Dec. 8, 2006.

In evaluating the DP World transaction or others like it, it is appropriate to consider the extent to which the United States depends on foreign entities to secure its supply chain. CSI depends on the cooperation of the host government of the overseas port of loading to inspect U.S. bound cargo. C-TPAT depends on the cooperation of overseas manufacturers and overland carriers to protect U.S. bound shipments from terrorist infiltration. ISPS relies on the cooperation of foreign governments and foreign-flag carriers to enforce port and vessel security codes. As one maritime industry spokesperson stated:

> This is an international business with an international problem. The only way it's going to be addressed effectively is through international efforts, which means the U.S. isn't going to do it all, nor can it do it all.[31]

Assessing DHS Maritime Security Initiatives

While the DP World issue spotlighted the role of terminal operators in port security, the initial debate about who should be operating U.S. ports quickly broadened into a debate about whether U.S. ports are secure. The DP World controversy refueled debate about whether the nation is doing enough, doing it with enough urgency, and spending enough on U.S. port and maritime security.[32] Members of Congress have referred to ports as the "soft underbelly" in U.S. homeland security,[33] to the shipping container as a modern day "Trojan horse,"[34] and have argued that there are still "massive blind spots" in the maritime security regime.[35] While no one asserts that enough has already been done to strengthen security, post-9/11 initiatives like CSI, ATS, C-TPAT, MTSA, and ISPS have, most acknowledge, created a framework for building a maritime security regime.

An issue of likely interest to Congress is the effectiveness of these maritime security initiatives. GAO has issued a number of reports addressing post-9/11 security initiatives. GAO has reported several factors limiting CSI, including staffing imbalances and lack of technical requirements for NII equipment used at foreign ports.[36] A number of concerns have also been raised by GAO regarding the C-TPAT

---

[31] Interview with Christopher Koch, World Shipping Council, *Journal of Commerce,* April 3, 2006, p. 44.

[32] For further background information on this debate, see CRS Report RL31733, *Port and Maritime Security: Background and Issues for Congress,* by John F. Frittelli, and CRS Report RS21293, *Terrorist Nuclear Attacks on Seaports: Threat and Response,* by Jonathan Medalia.

[33] Senator Dianne Feinstein as quoted in "Improved Security at Ports Urged," *Los Angeles Times,* February 24, 2005, p. 4.

[34] Statement of Senator Carl Levin, "Securing Global Supply Chain or Trojan Horse?" *States News Service,* May 26, 2005.

[35] Interview with Senator Norm Coleman, *Fox News Network,* March 28, 2006.

[36] See GAO testimony before the Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, *Homeland Security: Key Cargo Security Programs Can be Improved,* May 26, 2005, and *Container Security: A*

(continued...)

program including the scope of effort and level of rigor applied to the validation process; how many and the types of validations that are necessary to manage security risk; and various staffing issues.[37] The ATS system and CBP's targeting strategy more generally have been scrutinized by GAO in reports that criticize the strategy for not incorporating all the key elements of a risk management framework, and not being entirely consistent with recognized modeling practices.[38] Also, the DHS Inspector General published the results of an audit of CBP's targeting procedures, and concluded that improvements were needed regarding the data used by ATS, examination results should be used to refine ATS targeting rules, and physical controls over containers could be improved.[39] The DHS Inspector General has also raised concerns about the effectiveness of port security grants.[40] The GAO has also identified difficulties in deploying radiation scanners at U.S. ports[41] and it has reviewed the Coast Guard's ability to use risk management to guide its port security mission.[42] The CBP and Coast Guard have begun implementing many of the GAO's and OIG's recommendations.

Prioritizing Maritime Security Risks

A major concern for policymakers is assessing what is most at risk in the maritime domain and allocating the nation's resources accordingly. Three significant security issues in the container supply chain have been identified: (1) the integrity of the container packing process at the overseas factory or warehouse, (2) the integrity of the subsequent truck movement from the factory or warehouse to the overseas port of loading, and (3) the integrity of the manifest information that CBP uses, in part,

---

[36] (...continued)
Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts, GAO-05-557, April 26, 2005.

[37] See, GAO, *Homeland Security: Key Cargo Security Programs Can Be Improved*, GAO-05-466T, Testimony by Richard M. Stana, Director, Homeland Security and Justice Issues, before the Senate Permanent Subcommittee on Investigations, Committee on Homeland Security and Governmental Affairs, May 26, 2005.

[38] See, GAO, *Summary of Challenges Faced in Targeting Oceangoing Cargo Containers for Inspection*, GAO-04-557T, March 31, 2004 and *Cargo Container Inspections: Preliminary Observations on the Status of Efforts to Improve the Automated Targeting System*, GAO-06-591T, March 30, 2006.

[39] See, DHS OIG, *Audit of Targeting Oceangoing Cargo Containers (Unclassified Summary)*, OIG-05-26, July 2005.

[40] See, DHS OIG,, *Follow Up Review of the Port Security Grant Program*, OIG-06-24, February 2006, and *Review of the Port Security Grant Program*, OIG-05-10, January 2005.

[41] See, GAO, *Combating Nuclear Smuggling: DHS Has Made Progress Deploying Radiation Detection Equipment at U.S. Ports-of-Entry, but Concerns Remain*, GAO-06-389, March 2006.

[42] See, GAO, *Risk Management: Further Refinements Needed to Assess Risks and Prioritize Protective Measures at Ports and Other Critical Infrastructure*, GAO-06-91, December 2005.

to target high risk shipments for inspection.[43] Because there is no fool-proof way to address these vulnerabilities, some security experts call for greatly increasing the percentage of containers that are physically inspected. Others question whether a determined terrorist would not be able to find an inexpensive solution to circumvent screening technology.

While the threat of a shipping container being used as a "Trojan horse" by terrorists has received much attention, debate persists about the likelihood that terrorists would use them for such purpose. The GAO reports that while shipping containers are vulnerable, an extensive body of work by the FBI, academic, think tank, and business organizations concluded that the likelihood of such use to smuggle a weapon is considered low.[44] Some contend that a more likely tactic is that terrorists would attempt to smuggle a weapon using private watercraft and land at a public marina because they could remain in control of the weapon and avoid the scrutiny that occurs at official ports of entry. Terrorists could also smuggle a weapon in other types of cargo, such as motor vehicles or breakbulk cargo. They could repeat the attack method used against the *USS Cole* or the *Limberg* in which terrorists rammed a small boat packed with explosives into the hulls of these ships. They could employ this tactic against a cruise ship, a ferry, or a ship carrying hazardous cargo.[45]

The issue for Congress is how to protect U.S. ports and the supply chains on which the U.S. economy depends. Congress faces pressing questions about the overall security of ports and maritime commerce; the amount of funding that will be required to secure the maritime transportation system; and the amount of federal presence in ports that is necessary to prevent or deter terrorist use of ports as a destination or transit point for attacks on the United States.

---

[43] For a discussion of other maritime security issues, see CRS Report RL32841, *Border and Transportation Security: Possible New Directions and Policy Options*, by William H. Robinson, Jennifer E. Lake, and Lisa M. Seghetti.

[44] GAO-05-404, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, March 2005, p. 6-7.

[45] For further analysis on this issue, see CRS Report RL33787, *Maritime Security: Potential Terrorist Attacks and Protection Priorities*, by Paul W. Parfomak and John Frittelli.