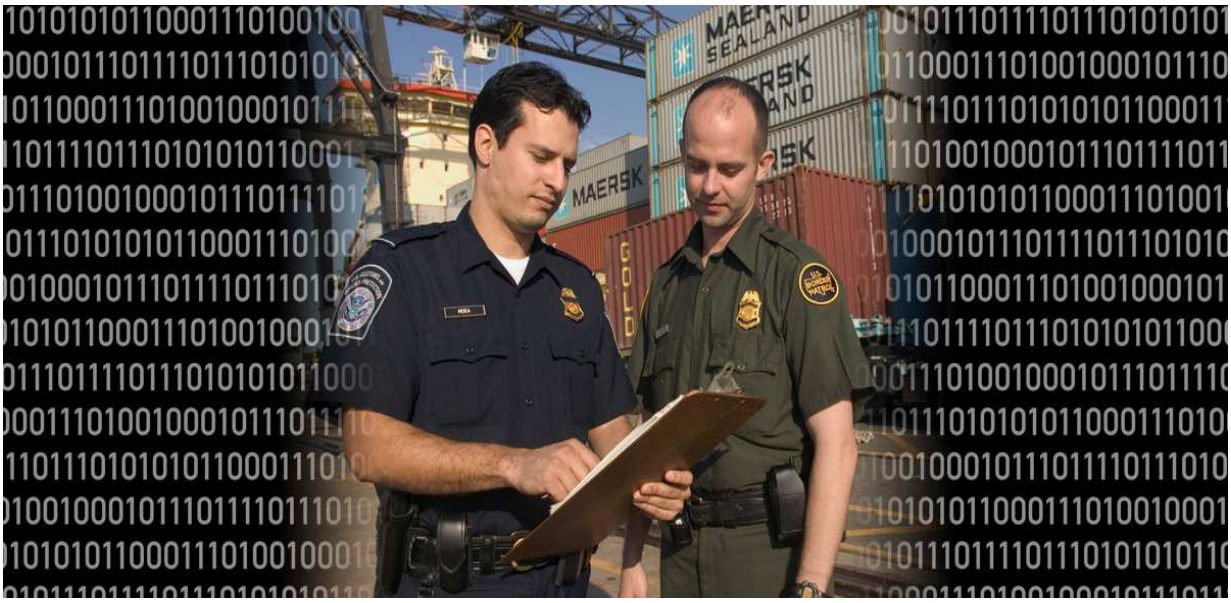
Port Security:
Guarding America's Front Door
A Town Hall Primer



Ninth Annual CITT State of the Trade and Transportation Industry Town Hall Meeting

Wednesday, February 7, 2007
6:00-8:30 PM

By
Thomas O'Brien, Ph.D.
with Allyson Clark,
California State University, Long Beach

Center for International Trade and Transportation

University College & Extension Services
California State University, Long Beach
The Choice for Continuing Education & Professional Development

METRANS Transportation Center
USC CSULB

Ninth Annual CITT State of the Trade and Transportation Industry Town Hall Meeting

Port Security: Guarding America's Front Door

Wednesday, February 7, 2007, 6:00 - 8:30 PM
Carpenter Performing Arts Center, CSULB

Agenda

Call to Order		Marianne Venieris, CSULB
Welcome Remarks		Dr. F. King Alexander, CSULB
Welcome Remarks		Mike Mitre, ILWU
Video Presentation	***A pictorial summary of cargo security measures and initiatives that have been implemented since 9-11***	
Keynote Introduction		Dr. Genevieve Giuliano, USC/METRANS
Keynote Address		Hon. Michael P. Jackson, Department of Homeland Security
Stakeholder Panel Discussion		
Moderator/Facilitator		Richard Hollingsworth, GCPI
➢ U.S. Customs & Border Protection		Todd Hoffman
➢ U.S. Coast Guard		Capt. Paul Wiedenhoeft
➢ Transportation Security Administration		John Schwartz
➢ FBI – Los Angeles		Ethel McGuire
➢ Private Sector/Boeing		Kenneth Konigsmark
Question & Answer Session with the Audience		
Closing remarks		Dr. Domenick Miretti, ILWU
Adjourn		Marianne Venieris

For more information, check our website at www.uces.csulb.edu/citt.

DISCLAIMER

The opinions and conclusions expressed or implied in the report are those of the author. They are not necessarily those of the METRANS Transportation Center, the Center for International Trade and Transportation, the US Department of Transportation or the California Department of Transportation.

Table of Contents

1. Securing the Supply Chain

In the wake of 9/11 the security landscape changed. New agencies were formed; and others took on added responsibility as officials in Washington, Sacramento and in Southern California determined who was responsible for keeping the nation safe. This was particularly the case for the agencies involved in securing our ports and the entire supply chain.

The security of the supply chain is the responsibility of agencies at the federal, state and local levels and of the industry stakeholders involved in moving goods. The largest governmental role falls to the federal government. The Coast Guard, Customs and Border Protection (CBP), and the Transportation Security Administration (TSA) - all part of the Department of Homeland Security (DHS) - play significant roles. Other federal agencies with a hand in port security include the Maritime Administration (MARAD) and Federal Bureau of Investigation (FBI).

The Coast Guard evaluates, boards, and inspects commercial ships as they approach U.S. waters. Customs and Border Protection is responsible for inspecting containers and for examining and inspecting ship crews and cruise ship passengers arriving in U.S. ports. CBP also pre-screens U.S.-bound containers at selected foreign ports. The Transportation Security Administration works with CBP to verify the contents of containers at their point of origin and track their movement from origin to destination. TSA, along with the Coast Guard, will also be responsible for overseeing the Transportation Worker Identification Credential (TWIC), a smart card which will be used to control access to secure areas of ports.

MARAD is part of the U.S. Department of Transportation. It publishes Maritime Security reports and makes recommendations on how best to ensure the security of containerized transportation. The FBI helps to coordinate law enforcement efforts in conjunction with other agencies including the Coast Guard and several area police forces as part of the local Joint Terrorism Task Force (JTTF). The JTTF has responsibility for disrupting terrorist plots.

The State is also involved in port security. The recently created California Maritime Security Council is charged with identifying threats, improving security measures, coordinating information and developing a statewide maritime security strategy. At the local level, an Area Maritime Security Committee comprising the FBI, police and fire departments, port executives and other agency representatives, helps identify needs for multi-agency cooperation and coordinated responses to port security matters. In September 2006, the Port of Long Beach approved the construction of a new Security Command and Control Center for various agencies from all levels of government.

These agencies reply upon other stakeholders, including ports, terminal operators and longshoremen, to identify security needs as well as test and implement security measures including the TWIC card. The Department of Homeland Security helps fund these on-the-ground efforts through the Port Security Grant program.

Security doesn't end at the terminal gate. The trucking community plays an active role in securing the supply chain as part of the federal Highway Watch program, which trains drivers to identify suspicious activity and potential security lapses while on the road.

This White Paper further investigates the role of these different stakeholders in developing policy and implementing technology in the service of port security. It also includes a timeline of events to show the transformation of their roles and responsibilities since 2001. Finally, there is a glossary of key security-related terms to help clarify what can often be a confusing topic.

The Legislative and Policy Environment: Roles and Responsibilities

The primary responsibility for securing the nation's ports rests with the federal government. This includes 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). The Maritime Administration (MARAD) of the US Department of Transportation also plays a critical role. Given the unique circumstances of different ports in different states, governmental agencies at state and local levels are increasingly playing a role in developing policy. This section considers those roles and responsibilities, the key pieces of legislation guiding the efforts of supply chain stakeholders and the role of technology in keeping ports secure.

The Role of the Federal Government: Reorganization Post 9-11

In November 2002, the US Congress approved the largest reorganization of government since World War II. It created a new Department of Homeland Security out of 22 different government agencies. In early 2003, the new department took responsibility for all border and security inspection functions previously carried out by the Immigration and Naturalization Service, the Border Patrol, and Customs Service; around the same time the Coast Guard was reorganized under DHS from the Department of Defense. Today, Homeland Security oversees the large majority of security efforts tied to both airports and maritime ports through three of its agencies: the Coast Guard, Customs and Border Protection, and the Transportation Security Administration.

The *Coast Guard* is responsible for evaluating, boarding, and inspecting commercial ships as they approach U.S. waters, relying upon intelligence from a variety of sources to provide a more complete picture of potential maritime security threats. It also tracks vessels to monitor ship traffic in harbors using Automatic Identification Systems.

The Coast Guard also oversees reporting requirements for ships entering and leaving U.S. ports. The Coast Guard requires foreign-flagged vessels and all commercial vessels entering a U.S. port from a foreign port to give a 96-hour advance notice of arrival (NOA). Prior to 9-11, the lead time for advance notification was only 24 hours. The NOA requires electronic submission of cargo manifest information to the National Vessel Maritime Center where it is screened via computer for suspicious activities. This allows the Coast Guard to identify in advance vessels that pose a potential risk.

Customs and Border Protection is responsible for inspecting cargo, including containers, and for examining and inspecting ship crews and cruise ship passengers arriving in U.S. ports. CBP also pre-screens U.S.-bound containers at certain foreign ports. Since October 2002, information on shipments is transmitted electronically to CBP 24 hours before cargo is loaded at a foreign port onto a U.S.-bound vessel. Before 9-11, carriers did not have to submit this information until the ship arrived in the U.S.; and the information was provided on paper manifests. Today CBP relies upon high tech systems to identify high-risk containers for physical inspection.

The *Transportation Security Administration* is most often associated with security at airports; but its responsibility includes cargo and passenger transport as well. Together with the CBP, TSA implements Operation Safe Commerce (OSC) which began in November 2002. OSC attempts to verify the contents of containers at their point of origin, ensure the physical integrity of the containers in transit, and track their movement from origin to destination over all modes of transportation.

TSA is also the agency, in conjunction with the Coast Guard, responsible for the Transportation Worker Identification Card (TWIC). The purpose of the TWIC is to control access to secure areas of passenger and cargo facilities. The card will use biometrics for a secure positive match of the individual to authorized locations.

The other key agency involved in port security at the federal level is the *Maritime Administration (MARAD)* of the U.S. Department of Transportation. MARAD publishes Maritime Security reports and a planning guide on security. MARAD is also responsible for making recommendations on how best to ensure the security of maritime container transportation and has developed a curriculum for training maritime security personnel.

These federal agencies are also key interfaces with international agencies with a hand in port security. The International Maritime Organization (IMO) developed the International Ship and Port Security Code (ISPS) which requires the installation of worldwide satellite tracking equipment, Ship Security Alert Systems, and radio vessel tracking devices to monitor a vessel's position.

The World Customs Organization (WCO) works to simplify customs procedures so that security standards do not unnecessarily disrupt the flow of trade. In May 2005, the WCO issued its Framework of Standards to Secure and Facilitate Global Trade. This document sets out principles for advance, electronic reporting of cargo and shipper information and requires importers to verify security measures taken by suppliers.

The Role of the Federal Government: Legislative Mandates and Security Processes

The roles and responsibilities of these various federal agencies have been set forth in a series of legislative mandates implemented since September 11, 2001.

Trade Act of 2002 (P.L. 107-210) The Trade Act gave the President increased authority to liberalize trade with other nations, but it also required exporters to electronically provide advance cargo data. According to US Census regulations, the electronic export manifest information cannot be shared with any country or private entity. The CBP requires this type of information from other countries, but the U.S. cannot reciprocate under current Census Bureau rules.

Maritime Transportation Security Act of 2002 (P.L. 107-295) The Marine Transportation Security Act requires the Coast Guard to develop national and regional area maritime transportation security plans. It requires ports, terminals, and certain types of vessels to develop security and incident response plans with approval from the Coast Guard. The Act also allows CBP to require electronic transmission of cargo manifest information prior to the arrival or departure of the cargo. The Act also requires the issuance of biometric security cards and the completion of background checks for entry into secure areas of maritime facilities or vessels. A controversial provision requiring user fees to pay for the cost of increased security was dropped from the bill in the conference committee.

Homeland Security Act of 2002 (P.L. 107-296) This piece of legislation, passed in November 2002, established the Department of Homeland Security as an executive department, combining 22 separate agencies with responsibility for monitoring borders, rails, airways, seaports, and customs. The Act called for DHS to prevent terrorist attacks within the United States; reduce the vulnerability of the United States to terrorism; and minimize the damage, and assist in the recovery, from terrorist attacks that do occur within the United States.

Coast Guard and Maritime Transportation Act (MTSA) of 2004 (P.L. 108-293) The Coast Guard and Maritime Transportation Act contains a number of provisions related to maritime security that add specificity to provisions of the Maritime Transportation Security Act. The Act requires the DHS to develop a plan for port security grants and how to allocate the funds. The Act also requires the U.S. Department of Transportation to evaluate sensors that can track marine containers, and detect hazardous and radioactive materials inside containers.

Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) The Intelligence Reform and Terrorism Prevention Act imposes deadlines for a transportation worker card deployment plan, the preparation of a national maritime security plan, completion of facility and vessel vulnerability assessments, status report on seafarer identification, and a status report on establishing performance standards for container seals and locks. The Act also requires DHS to develop a terrorism “watch list” for passengers and crews aboard cruise ships.

Security and Accountability for Every Port (SAFE Port) Act of 2006 (P.L. 109-347) The SAFE Port Act authorizes $3.4 billion over five years to implement security programs, including $400 million for port security grants. The legislation codifies and expands some key security measures previously launched. These include the Container Security Initiative (CSI) which deploys American inspectors at foreign ports. SAFE Port also clarifies the definition of security risk and establishes an ambitious timeline for implementation of a transportation worker ID card. It calls for the top 10 US ports (including Long Beach and Los Angeles) to begin using access cards by July of 2007.

One of the goals of these various legislative efforts has been to standardize formerly non-standardized security processes; or as in the case of the 24-hour and 96-hour rules, tighten existing regulations. The first major attempt was the Customs-Trade Partnership Against Terrorism (C-TPAT) which was initiated in April of 2002. C-TPAT offers importers expedited processing of cargo if they comply with CBP guidelines for securing their entire supply chain. To be a partner in C-TPAT, an importer must complete a detailed questionnaire on its security practices, list all the partners in its supply chain, and confirm that these other firms also have security programs in place. If certified by CBP, importers may benefit from a reduced number of cargo inspections.

Studies have determined that there are a number of problems with C-TPAT that need correction.[1] A General Accounting Office (GAO) study found that importers participating in C-TPAT were benefiting from reduced scrutiny of their cargo after they had been certified into the program but before CBP had validated that they were in fact carrying out the promised security measures. GAO also found that nearly one-third of the containers that CBP had targeted for inspection at overseas loading ports – including those labeled "high-risk" – were not actually inspected.[2]

Another procedural change, this time making use of technology, is the Container Security Initiative (CSI). CSI was first announced in January of 2002, is implemented by Customs and Border Protection, and deploys American inspectors at foreign ports. Some 70% of all containers arriving in California do so under provisions of the CSI.

CSI consists of four core elements:

1) Using intelligence and automated information to identify and target containers that pose a risk for terrorism.

2) Pre-screening those containers that pose a risk at the port of departure before they arrive at U.S. ports.

3) Using detection technology to quickly pre-screen containers that pose a risk.

---

[1] GAO, Homeland Security: Key Cargo Security Programs Can Be Improved, GAO-05-466T, May 26, 2005. (http://www.gao.gov/new.items/d05466t.pdf)
[2] DailyBreeze.com, June 3rd, 2005

4) Using smarter, tamper-evident containers.

CBP uses a system known as the Automated Targeting System (ATS) to identify high-risk containers for physical inspection. These are containers that may involve smuggling or pose a potential terrorism threat. The CBP is now requiring more detailed information in order to minimize the need for examination holds in U.S. ports. CBP created the 24-hour rule to allow targeting of "suspicious cargo" and a possible "no load" order at the foreign port of lading. By "extending the borders," CBP minimizes the risk of a dirty bomb or other device detonating in U.S. ports.

In its first 3 years, 26 customs administrations committed to joining CSI and are at various stages of implementation. CSI is now operational at ports in North America, Europe, Asia, Africa, the Middle East, and Latin and Central America. CBP's goal was to have 50 operational CSI ports by the end of fiscal year 2006, with approximately 90 percent of all transatlantic and transpacific cargo imported into the United States subject to prescreening.

Sometimes the procedural changes pursued by the federal government targeted the often complex and cumbersome working arrangements between different organizations. New programs encouraged different agencies with different areas of expertise to work together. One such example is the Secure Freight Initiative. This program was developed by the Department of Homeland Security and the Department of Energy in 2006. It has established an International Container Scanning Network involving partnerships between US and foreign ports to install radiation detectors and imaging equipment at terminals around the world. Combined with an effort to upgrade the electronic manifest tracking process, containers will undergo intensive scrutiny before setting sail for the United States.

Sometimes the procedural changes are designed to encourage more public-private partnerships. In addition to C-TPAT, which is one of the largest public-private efforts of any type since 9-11, there is also Operation Safe Commerce (OSC). Launched in late 2002 by the US Department of Transportation along with Customs, Operation Safe Commerce encouraged collaborative efforts between the federal government, the business community and the maritime industry. The goal was to develop and share best practices for the safe movement of containerized cargo.

OSC originally identified 18 projects at the ports of Los Angeles/Long Beach, New York/New Jersey, and Seattle/Tacoma which examined technologies and practices while testing innovative solutions. The projects involved scrutinizing supply chain security through container tracking and tracing technology, non-intrusive detection strategies and improved container seal concepts.

The Role of the Federal Government: Deploying New Technologies

Apart from changes in processes and procedures, the new security landscape has brought about changes in the way technology is used at the ports and along the supply chain. The federal government has played a central role in both developing standards and funding deployments.

One example used by Customs and Border Protection is the mobile Vehicle and Cargo Inspection System (VACIS), which consists of a truck-mounted, non-intrusive gamma ray imaging system that produces radiographic images to evaluate the contents of trucks, containers, cargo, and passenger vehicles. VACIS exams help to determine the possible presence of many types of contraband. With VACIS, CBP is able to verify that the goods declared via electronic manifest systems are in fact in the container.

Another technological tool increasingly used by CBP is the Radiation Portal Monitor (RPM). An RPM provides Customs and Border Protection with a passive, non-intrusive means of screening containers for the presence of nuclear and radiological materials. An RPM can detect various types of radiation emanating from nuclear devices, dirty bombs, special nuclear materials, and natural sources and isotopes commonly used in medicine and industry.

On a daily basis, ports of Los Angeles and Long Beach receive 11,000 containerized imports. All of the containers that leave the terminals by truck are scanned by one of the 85 portal radiation monitors in place at the 13 container terminals. The Port of Oakland was the first seaport in the country to implement portal monitors in April of 2005.

Perhaps the most controversial technology tool being discussed is the Transportation Worker Identification Credential (TWIC). The TWIC prototype is currently being tested at maritime, rail, aviation and ground transportation facilities in California (Los Angeles/Long Beach area), Florida, Pennsylvania, New Jersey, New York and Delaware.

A secure worker identification card was first authorized in 2001. The development and issuance of biometric security cards was subsequently addressed in 2002 and 2004 as part of the marine transportation security legislation addressed above.

The TWIC is a proposed “smart” photo ID card with multiple fraud protection measures. It is expected to cover up to 850,000 longshoremen, truckers, merchant mariners and other port workers requiring unescorted access to facilities and vessels across the country. Facility owners, operators and unions will submit information on workers to the Transportation Security Administration. The TSA will check the names against terrorist watch lists and criminal records, and perform citizenship and immigration service checks. The cost of the card will be paid by the worker; reduced costs are available to those workers who have already undergone comparable background checks. Cards will be valid for five years.

TWIC was one of the programs specifically addressed by the Security and Accountability for Every Port (SAFE Port) Act that the President signed in October of 2006. The legislation clarifies the definition of security risk and it establishes an ambitious timeline for TWIC implementation. It calls for the top 10 US ports (including Long Beach and Los Angeles) to begin using access cards by July of 2007.

There has been some resistance to TWIC from ports, marine terminals, and drivers and longshoremen who will be required to obtain the card. From the port and terminal perspective, the concerns primarily have to do with time and money. TWIC regulations require port officials and the Coast Guard to work together to designate secure areas within facilities as well as in and around vessels. They will have to integrate TWIC access technology with existing control systems. Officials have also expressed concerns whether the system will be flexible enough to quickly credential a casual or part-time worker.

Proposed TWIC regulations state that a transport worker can be denied access if (s)he has been convicted of a felony within the past seven years. The SAFE Port Act narrowed the list of offenses to treason, espionage, sedition and terrorism. Union leaders want to be certain that violations that don't necessarily compromise security won't disqualify an applicant. The impact of immigration checks on the port drayage industry is unknown.

The Role of State and Local Government

While the lion's share of port security measures are directed by the federal government, there are efforts underway by state and local government to supplement those efforts or fill in the gaps. In late 2006, Governor Schwarzenegger signed an executive order creating the California Maritime Security Council. The Council includes representatives of Homeland Security, the U.S. Coast Guard, the U.S. Navy, state agencies and harbor businesses and labor unions. Action items for the council include identifying threats, improving security measures, coordinating information and developing a statewide maritime security strategy.

Local government works in conjunction with agencies at higher levels of government. The Federal Bureau of Investigation has established a Long Beach Resident Agency with 16 full time special agents who monitor and help coordinate law enforcement efforts in a Joint Terrorism Task Force. The local JTTF has responsibility for disrupting terrorist plots and relies on the coordination of Federal and local agencies, including the Coast Guard and several area police forces.

Additionally, the FBI joins with the Coast Guard as co-coordinators of the Area Maritime Security Committee. This Committee was established in 2004 and comprises the FBI, Police and Fire Departments, Port executives and other agency representatives. It helps identify needs for multi-agency cooperation and coordinated responses to port security matters. The Port of Long Beach in 2006 approved the construction of a new Security Command and Control Center for various agencies from all levels of government.

Non-governmental Response: Funding for Changing Industry Practices

Despite the central role played by government at all levels, often the most dramatic impact of the new security regime is felt by the operators on the ground: the ports, the terminal operators, the truckers and the longshoremen. These stakeholders are expected to implement the technology and procedures designed by government. They are also expected to be the eyes and ears of a secure supply chain.

Truck drivers for example, take part in a program called Highway Watch which trains drivers to identify suspicious activity and potential security lapses while on the road. These include abandoned rigs and trucks parked under bridges. Transportation companies, in conjunction with warehouses and other logistics industry stakeholders have formed an American Logistics Aid Network (ALAN). ALAN was established in the wake of Hurricane Katrina and the Indian Ocean Tsunami to coordinate the collection, routing, and delivery of supplies in response to a disaster. It offers a model of coordination and cooperation across modes and industry segments if the supply chain is threatened.

Industry experimentation is also underway in the utilization of Radio Frequency Identification Devices (RFID) attached to containers for tracking purposes. Shipping companies recognize that tracking, evaluating and inspecting suspicious cargoes at the points of origin, before loading those goods on ships, is an important part of defeating terrorism. RFID e-seals on containers are a good example. Normal seals simply check for mechanical integrity, but a determined criminal can bypass the seal by removing an entire door with the seal intact. E-seals allow for cost-effective monitoring from origin to destination. E-seals also can contain the container number, potentially making error-prone optical character recognition (OCR) systems obsolete. The container number recorded on the e-seal can be matched to a container number in a secure database to reveal the contents and other information about the cargo.

Most security efforts however have been directed by the ports and terminals; and both the Ports of Los Angeles and Long Beach are developing security plans. The ports and terminals are working to increase surveillance, fencing, lighting, training, and patrols. The Ports of Long Beach and Los Angeles and the Alameda Corridor Transportation Authority are implementing the Advanced Transportation Management, Information and Security (ATMIS) System which will include closed circuit television surveillance, changeable message signs, and queue detectors to help manage traffic flow and to increase security. The $7.8 million program is projected to be operational by November of 2008. The Port of Long Beach is also outfitting 16 harbor patrol cars with camera systems that can transmit video and live feeds to central command centers.

The problem comes in paying for government-mandated security measures or measures designed by the port facilities themselves. In earlier rounds of port security grants from Washington, the Ports of Los Angeles and Long Beach together received only a third of what had been requested.

The Department of Homeland Security awarded a new round of port security grants in September 2006. $168 million was allocated to ports grouped into one of four tiers, with

Tier 1 representing the highest risk. The Ports of Long Beach and Los Angeles received a combined $12 million in this cycle. $11.6 million went to the Port Authority of New York and New Jersey with Louisiana ports also receiving significant grants. San Francisco and Oakland received no money as part of the 2006 grants; Oakland had requested $6 million in federal funding. The Port of Richmond received almost $1.2 million. Florida and Texas among other states have reportedly been successful in coordinating multiple state port security grant applications using a clearinghouse approach, and thereby increasing overall state grant awards. California has no such mechanism.

Of the San Pedro Bay Ports' 12 million, $4.6 million earmarked for the Port of Los Angeles will be used to begin implementing the TWIC program at the Port. While the SAFE Port Act authorizes $3.4 billion over five years to implement security programs, including $400 million for additional port security grants, the legislation is less specific about funding sources for security programs. Rather, it codifies and expands some key security measures previously launched.

With limited dollars available and so much at stake, it is critical that the various agencies involved with port and maritime security work together to avoid overlap, duplication of effort and conflicting regulations. There also needs to be greater sharing of intelligence information among federal, state and local agencies. In bringing together representatives from the various port stakeholders and agencies, the 9th Town Hall hopes to facilitate that process.

2. Timeline of Port-Related Security Events

2001

After September 11, 2001 The Southern California Marine Transportation System Advisory Council (SOCAL-MTSAC) develops security protocols that allow the ports to stay open and productive after 9/11.

November 1, 2001 U.S. Customs Commissioner announces the implementation of the Customs Trade Partnership Against Terrorism or C-TPAT. The Partnership involves worldwide customs agencies working with international shipping companies to improve standards for goods movement. Companies that comply with C-TPAT standards receive expedited customs processing.

November 19, 2001 Aviation and Transportation Security Act of 2001 first authorizes a secure transportation worker identification card.

2002

November 19, 2002 House and Senate approve largest reorganization of government since WWII by creating Department of Homeland Security out of 22 different government agencies.

November 20, 2002 U.S. Department of Customs and U.S. Department of Transportation announce the launch of the Operation Safe Commerce Program to provide a test-bed for new security techniques that have the potential to increase the security of container shipments.

November 25, 2002 George Bush signs into effect the Maritime Transportation Security Act of 2002 (MTSA). It is designed to protect the nation's ports and waterways from a terrorist attack and requires vessels and port facilities to conduct vulnerability assessments and develop security plans that may include passenger, vehicle and baggage screening procedures; security patrols; establishing restricted areas; personnel identification procedures; access control measures; and/or installation of surveillance equipment.

December 2, 2002 Implementation of 24 hour cargo manifest rule begins, requiring carriers to submit a declaration 24 hours before cargo is loaded aboard a vessel at a foreign port.

December 13, 2002 The International Maritime Organization (IMO) conference adopts International Ship and Port Facility Security Code (ISPS). Contracting governments ensure completion of a Port Facility Security Assessment, and identify the level of risk for each port facility within its territory that serves ships engaged in international voyages. Facilities are also required to appoint a Port Facility Security Officer and prepare a Facility Security Plan.

2003

January 30, 2003 DHS announces the combination of all border security and inspection functions previously carried out by the Immigration and Naturalization Service (INS), the Border Patrol, the Customs Service, and the Animal and Plant Health Inspection Service of the Department of Agriculture.

February 25, 2003 Coast Guard reorganized under Department of Homeland Security from the Department of Defense. Duties include protecting ports, the flow of commerce, and the marine transportation system from terrorism; and to maintain maritime border security.

July 1, 2003 The President's fiscal year 2004 budget request to Congress includes $34 million for Maritime Intelligence.

November 19, 2003 Transportation Security Administration meets deadline to have more than 47,000 airport security workers in place at 424 airports.

December 17, 2003 President Bush signs Homeland Security Presidential Directive Number 7 (HSPD7). The directive establishes a national policy to identify and prioritize the United States' critical infrastructure.

2004

August 9, 2004 President Bush signs into law H.R. 2443, the Coast Guard and Maritime Transportation Act of 2004. The Act authorizes appropriations for the United States Coast Guard, facilitates navigation and shipping, and strengthens the security of maritime transportation.

2005

April 26, 2005 The Port of Oakland and U.S. Customs and Border Protection (CBP) demonstrate Radiation Portal Monitor systems at the Oakland seaport's seven international terminals. The twenty-five portals screen all international container traffic exiting the Port for sources of radiation.

2006

July 11, 2006 President Bush signs into law H.R. 889, the Coast Guard and Maritime Transportation Act of 2006. The Act authorizes money for projects including bridge alteration and removal.

September 1, 2006 Department of Homeland Security awards FY 2006 port security grants. The Ports of Los Angeles and Long Beach receive a combined $12 million.

October 13, 2006 President Bush signs H.R. 4954, the SAFE Port Act, including requirement that all cargo entering the country's 22 busiest ports be scanned for radiation by the end of 2007. The Act also establishes an ambitious timeline for implementation of TWIC and allocates risk-based funding through grants to help harden U.S. ports against terrorist attacks.

2007

January, 2007 The Department of Homeland Security (DHS) expected to launch the first phase of the Secure Freight Initiative. The $60-million program is expected to enhance the ability of the United States to scan containers abroad for nuclear and radiological materials and to increase risk assessment of U.S.-bound containers. The first phase involves the deployment of a combination of nuclear detection devices to six foreign ports: Port Qasim, in Pakistan; Puerto Cortés, in Honduras; Southampton, in the United Kingdom; Port Salalah, in Oman; the Port of Singapore; and the Gamman Terminal at Port Busan, in Korea. The project is also being tested at a port in Hong Kong.

January 1, 2007 White House Office of Management and Budget approves the Transportation Worker Identification Credential rule.

January 3, 2007 Cargo Shippers lobby to derail a proposal for mandating inspections of all cargo.

March, 2007 Background checks expected to begin on an estimated 750,000 longshoremen, mariners and other port workers across the country.

3. Port Security Glossary

Advanced Transportation Management Information and Security (ATMIS)

Provides motorists leaving the Port Complex with "real time" traffic conditions and advanced warning of incidents in the vicinity of the Port.

Automated Secure Vessel Tracking System (ASVTS)

A secure Vessel Tracking System that employs satellite and AIS (Automatic Identification System) transmissions and other sources of information to track the locations of vessels.

California Office of Homeland Security

California's Homeland Security Strategic Directives are to mirror those identified in the national strategy, including prevent terrorist attacks within the State, reduce California's vulnerability to terrorism, and minimize the damage from attacks that do occur.

Coast Guard and Maritime Transportation Act of 2004

The Act requires the Department of Homeland Security to develop a plan for port security grants and how to allocate the funds; requires the U.S. DOT to evaluate sensors that can track marine containers and detect hazardous materials inside the containers.

Container Seal One-time guards against pilferage; make tampering readily apparent.

Container Security Initiative

Customs and Border Protection program intended to help increase security for containerized cargo shipped to the United States from around the world. Containers are prescreened and evaluated before leaving foreign port.

Customs and Border Protection (CBP)

Agency responsible for inspecting cargoes, including containers, and for examining and inspecting ship crews and cruise ship passengers arriving in U.S. ports from any foreign port.

Customs-Trade Partnership Against Terrorism

Federal program involving worldwide customs agencies working with international shipping companies to improve standards for goods movement. Companies that comply with C-TPAT standards receive expedited customs processing.

Department of Homeland Security (DHS)

Federal agency responsible for unifying homeland security objectives of more than 100 different governmental organizations.

Intelligence Reform and Terrorism Prevention Act of 2004

Directs the Transportation Security Administration to begin screening passengers and crews of cruise ships against comprehensive consolidated terrorist databases. Provisions include deployment of biometric entry and exit system.

International Maritime Organization (IMO)

International body which develops and maintains a comprehensive regulatory framework for shipping including safety, environmental concerns, legal matters, technical co-operation, and maritime security.

International Ship and Port Security Code (ISPS)

A comprehensive security regime that seeks to establish an international framework of co-operation between governments, government agencies and the shipping and port industries in order to detect and take preventive measures against security incidents affecting ships or port facilities used in international trade.

Joint Harbor Operations Center

Centers controlled by Navy and Coast Guard personnel who fuse radar, surveillance and intelligence data to create a layered defense of domestic ports. The centers' responsibility includes monitoring the movement of commercial deep-draft vessels and tug and barge combinations in waterways where both the Navy and Coast Guard use ports.

Joint Terrorism Task Force (JTTF)

Local taskforce with responsibility for disrupting terrorists plots; relies on the coordination of Federal and local agencies, including the FBI, Coast Guard and several area police forces.

Maritime Administration (MARAD)

MARAD, a division of the U.S. Department of Transportation, is charged with improving and strengthening the U.S. maritime transportation system—including infrastructure, industry and labor—to meet the economic and security needs of the Nation.

Maritime Transportation Security Act of 2002 (MTSA)

Imposes broad security requirements on the maritime industry by requiring comprehensive security plans for U.S. ports and mandated improved identification and screening of seaport personnel.

96-Hour Advance Notice of Arrival (96-Hour Rule)

The Coast Guard requires foreign-flagged vessels and all commercial vessels (foreign or domestic) entering a U.S. port or place from a foreign port to give a 96-hour advance notice of arrival (ANOA). It requires electronic submission of cargo manifest information to the National Vessel Maritime Center where it is screened via computer for suspicious activities. This allows the Coast Guard to identify vessels that pose any risk before entering the ports.

Operation Safe Commerce (OSC)

A program to fund business initiatives designed to enhance security for container cargo moving throughout the international transportation system.

Port Security Grant Program

Program administered by Department of Homeland Security to create sustainable, risk-based efforts for the protection of critical port infrastructure from terrorism; part of Infrastructure Protection Program. Ports to receive $201.2 million in security grants in fiscal year 2007.

Radio Frequency Identification (RFID)

Identification method, using radio waves and tags/transponders to store and remotely retrieve data; possible means of identifying and tracking cargo containers.

Radiation Portal Monitor (RPM)

Detection device that provides Customs and Border Protection (CBP) with a passive, non-intrusive means to screen containers and other conveyances for the presence of nuclear and radiological materials.

Security and Accountability for Every Port Act (SAFE Port Act)

Federal legislation adopted in 2006; requires that all cargo entering the country's 22 busiest ports be scanned for radiation by the end of 2007; calls for the top 10 U.S. ports (including Long Beach and Los Angeles) to begin using TWIC access cards by July of 2007.

Safety of Life at Sea Convention (SOLAS)

International Maritime Organization's SOLAS Convention is an international treaty concerning the safety of merchant ships; addresses safety of navigation, construction, carriage of cargo, and operation of ships. Makes mandatory ISPS code.

Trade Act of 2002

Also called the U.S. Trade Promotion Authority Act; grants the President of the United States the authority to negotiate trade deals with other countries and only gives Congress the approval to vote up or down on the agreement, but not to amend it.

Transportation Security Administration (TSA)

Division of the Department of Homeland Security responsible for security of the nation's highways, railroads, buses, mass transit systems, ports and the 450 U.S. airports. Together with the CBP, TSA oversees the Operation Safe Commerce (OSC) program.

24-Hour Rule

Requires sea carriers and NVOCCs (Non-Vessel Operating Common Carriers) to provide U.S. Customs with detailed descriptions of the contents of sea containers bound for the United States 24 hours before the container is loaded on board a vessel.

Transportation Worker Identification Credential (TWIC)

Proposed "smart" photo ID card with multiple fraud protection measures expected to cover up to 850,000 longshoremen, truckers, merchant mariners and other port workers requiring unescorted access to facilities and vessels across the country.

Vehicle and Cargo Inspection System (VACIS)

The mobile Vehicle and Cargo Inspections System (VACIS) is a gamma ray scanning system that captures an image of a marine container, rail car, or truck contents. It gives the operators of this equipment an image similar in many ways to an X-ray.

World Customs Organization (WCO)

The WCO is an independent intergovernmental body with 169-member governments whose mission is to enhance the effectiveness and efficiency of Customs administrations.

ACKNOWLEDGEMENTS

Funding to support the development of this White Paper was provided by the METRANS Transportation Center through grants provided by the US Department of Transportation and the California Department of Transportation. Input provided by the Policy and Steering Committee of the Center for International Trade and Transportation at California State University, Long Beach and the California Marine and Intermodal Transportation System Advisory Council is greatly appreciated. Particular thanks to Lawrence Mallon of Mallon and Associates for sharing his knowledge of maritime security and providing organizational direction. All errors and omissions are the responsibility of the author.

Sponsors:

United States Department of Transportation

Long Beach Business Journal

Price Transfer

USC Sea Grant

Industry Endorsements:

California Marine and Intermodal Transportation System Advisory Council • California Trucking Association • Foreign Trade Association • FuturePorts • Gateway Cities Council of Governments • Gateway Cities Partnership, Inc. • Harbor Association of Industry and Commerce • Harbor Transportation Club • International Business Association of Southern California • International Warehouse Logistics Association • Long Beach International Trade Office • Los Angeles County Economic Development Corp. • Los Angeles Custom Brokers and Freight Forwarders Association • Los Angeles Transportation Club • Propeller Club of Los Angeles-Long Beach • Women in International Trade Orange County • Women's Transportation Seminar Los Angeles • World Trade Center Association Los Angeles-Long Beach