California State Legislature

Joint Legislative Committee on
Emergency Services & Homeland Security

and

Senate Committee on Transportation & Housing
Subcommittee on California Ports & Goods Movement

Securing California's Maritime Transportation System: Seamless Operational Security (SOS)

Friday, August 11, 2006 • 1 p.m.
Long Beach Public Library Auditorium
101 Pacific Ave., Long Beach

Hon. Christine Kehoe, Chair
Joint Legislative Committee on Emergency Services
and Homeland Security

Hon. Alan Lowenthal, Chair
Senate Transportation & Housing Committee
Subcommittee on Ports & Goods Movement

1372-S

Joint Hearing

Joint Legislative Committee on
Emergency Services and Homeland Security
and the
Senate Committee on Transportation & Housing
Subcommittee on California Ports & Goods Movement

Securing California's Maritime Transportation System: Seamless Operational Security (SOS)

Friday, August 11, 2006
1:00 p.m. – 5:20 p.m.
Long Beach Public Library Auditorium
101 Pacific Avenue, Long Beach, CA

Agenda

Opening Remarks
Hon. Christine Kehoe, Chair, Joint Legislative Committee on Emergency Services and Homeland Security

Hon. Alan Lowenthal, Chair, Senate Transportation & Housing Committee, Subcommittee on Ports & Goods Movement

Hon. Pedro Nava, Vice Chair, Joint Legislative Committee on Emergency Services and Homeland Security

Members of the Committees

"Protecting the Nation's Seaports: Balancing Security and Cost"
Jon Haveman, Ph.D. Program Director, Public Policy Institute of California, Editor, "Protecting the Nation's Seaports: Balancing Security and Cost," issued June 28, 2006.

Special report on port security produced by KCET and aired May 5, 2006, during "California Connected."

How secure are California's ports today?
Captain Wiedenhoeft, Captain of the Port, San Pedro Bay Ports, U.S. Coast Guard

Gary Winuk, Chief Deputy Director, Governor's Office of Homeland Security

Cosmo Perrone, Director of Security, Port of Long Beach, representing California Association of Port Authorities (CAPA)

Transportation Worker Identification Credential (TWIC) Implementation
Mike Mitre, Director of Port Security, International Longshore and Warehouse Union

Where are the gaps?
Larry Mallon, Ph.D., Chair, AB 2043 CALMITSAC Port Security Study Committee – "Growth of California Ports: Opportunities and Challenges"

Captain Ralph Tracy, Chair, American Association of Port Authorities (AAPA) Security Committee

Noel Cunningham, Principal, The MARSEC Group

How has port funding been spent and what's in the future?
Gary Winuk, Chief Deputy Director, Governor's Office of Homeland Security

Should we fail in protecting our ports, what consequences can we anticipate, and what steps should California ports take now?
Jim Moore II, Ph.D., Professor of Industrial and Systems Engineering, Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California

Public Comment
If you wish to speak, please provide your contact information to the Sergeant-At-Arms and please limit comments to 3 minutes per person.

Adjournment

Table of Contents

Presentations during the hearing

Larry Mallon, Ph.D. Page 62
Chair, AB 2043 CALMITSAC Port Security Study Committee

- "California's First Comprehensive Port Security Survey and Capability Gap Analysis," Dr. Lawrence G. Mallon, Esq., California State University at Long Beach, and Captain Bruce Clark, USCG retired, California Maritime Academy, with assistance from San Diego State University Foundation."

James E. Moore, II, Ph.D. Page 134
Professor of Industrial and Systems Engineering, Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California.

- "Should We Fail to Protect Our Ports, What Consequences Should We Anticipate: Simulating the State-by-State Effects of Terrorist Attacks on Three Major U.S. Ports," Jiyoung Park, Professor Peter Gordon, Professor James E. Moore, II, and Professor Harry W. Richardson, Center for Risk and Economic Analysis of Terrorism Events (CREATE), University of Southern California, August 11, 2006.

Background Material Made Available to Committee Members Prior to the August 11, 2006 Hearing

- "The Maritime Infrastructure Recovery Plan for the National Strategy for Maritime Security, April 2006. Page 160

- FY2006 Infrastructure Grant Programs, U.S. Department of Homeland Security, Office of Grants and Training, Program Summary. Page 172

- 2005-2006 Legislation Related to Port Security. Page 206

- Data sheets on California's ports: Page 208
    1. The Port of Humboldt Bay, Eureka
    2. The Port of Stockton, Stockton
    3. The Port of Sacramento, West Sacramento
    4. The Port of Richmond, Richmond
    5. The Port of San Francisco, San Francisco
    6. The Port of Redwood City, Redwood City
    7. The Port of Hueneme, Port Hueneme
    8. The Port of Long Beach, Long Beach
    9. The Port of Oakland, Oakland
    10. The Port of Los Angeles, San Pedro
    11. The Port of San Diego, San Diego

Introduction and Background

On August 11, 2006, California State Senators Christine Kehoe and Alan Lowenthal convened a combined hearing of the Joint Legislative Committee on Emergency Services and Homeland Security and the Senate Committee on Transportation and Housing's Subcommittee on California Ports and Goods Movement. The subject of the hearing was "Securing California's Maritime Transportation System: Seamless Operational Security (SOS)," a determination of how secure the state's ports are, and findings and recommendations on improvements that could be made.

The hearing took place at the Long Beach Library, near the Port of Los Angeles and the Port of Long Beach, the first and second busiest container ports in the nation. Together with the Port of Oakland, the nation's fourth busiest container port, these three ports serve as points in global goods movement and combined handled about forty percent of the nation's container traffic in 2004.

In 2004, about 1.4 billion tons of freight moved through 361 American ports, according to a report issued by the Public Policy Institute of California (PPIC) in June 2006. Goods transported via containers are 59.3% of the total value of all U.S. maritime trade and 14.9% of its total volume. It is no wonder, then, that when security at the nation's ports is under discussion, cargo containers tend to be the major focus.

According to Dr. Jim Moore from the University of Southern California's Center for Risk and Economic Analysis of Terrorism Events (CREATE), in 2004 the Los Angeles and Long Beach ports represented seven percent of the region's labor force, with about 600,000 jobs and $243 billion in import and export trade, which represented 10% of U.S. trade. More importantly, half of all imports and two-thirds of all exports are to and from areas beyond the Los Angeles region. Consequently, should a terrorist event take place at one or both of these ports, the impacts most likely would be felt to some extent nationwide.

Shutting down such productive economic engines is an acknowledged prime target for terrorists. While both public and private efforts to secure ports and landside ports of entry occurred prior to September 11, 2001, it has been since then that federal, state and local governments, and the maritime industry have worked to improve the security of an industry that involves 40,000 companies worldwide in the container freight consolidation industry alone, 8 to 10 million workers worldwide, with 20 million ocean containers in transit in 2004.

Goods movement is important to both California's and the nation's economy. Many of the security enhancements in place at our seaports focus on cargo containers in transit to and from foreign ports as potential targets. In 2003, approximately $807 billion in goods moved through America's 361 seaports, representing 41% of the nation's international goods trade that year. The majority of America's major seaports are located in or near major population centers, and as a consequence, the people living in communities and

working in business districts surrounding our ports are also at risk. In California, that includes Long Beach, Los Angeles, Oakland, Sacramento, San Diego and San Francisco.

The Joint Legislative Committee on Emergency Services and Homeland Security has heard testimony over the past two years on how much of the nation's infrastructure is vulnerable to attacks by terrorists, both foreign and "home-grown." Ports are especially at risk given al-Qaeda's public pronouncements that destroying the American economy is its prime objective.

Past terrorist events ranging from the USS Cole bombing to September 11, subway attacks in Madrid and London, to the plan uncovered less than a day before this hearing by British intelligence to explode ten or more planes enroute from England to America, reinforce the importance of vigilance and preparedness in the daily lives of those who work in or around potential targets.

During the hearing, testimony indicated that prior to September 11, the nation's primary port security focus was in response to the 1985 hijacking of the Achille Lauro cruise ship in the Mediterranean Sea. Now, in the post September 11 world, port security plans are based on the potential for the transport of terrorists, a "dirty bomb" or the threat of a bioterrorist attack via the millions of containers that flow to and fro across America's borders annually.

A comprehensive strategic planning effort should include preparing for the multiple methods by which a terrorist could strike in or near one of the nation's 361 active ports. Perhaps the next attack will use small pleasure craft similar to the attack on the USS Cole; or come in on bulk carriers, on an oil tanker, a roll on/roll off, fishing trawler, or a vessel carrying timber or lumber.

The threat potential includes landside activities: the highways and train tracks leading to and from the ports pass through surrounding neighborhoods and business districts that are often densely populated. Panelists indicated that this is where the State of California can and should play a role. There is no agency with a better understanding of what is happening on our highways than the California Highway Patrol (CHP). The CHP has an active inspection program for trucks and identification procedures in place for truck drivers. It is the state that works closely with local government, and through the Office of Homeland Security (OHS) and the Office of Emergency Services (OES), has established intelligence networks, conducts training exercises, and develops funding strategies.

Ports may not always be the main target in an attack, and may suffer collateral damage leaving them unable to function because strategically located bridges are destroyed. Blocking ocean-going vessels, vital train connections and major goods movement corridors means that supply chains will break down. Should a disruption take place at the Ports of Los Angeles and Long Beach, an estimated two-thirds of the impact would be felt outside California.

Summary of the Hearing Testimony

Securing California's Maritime Transportation System: Seamless Operational Security (SOS)

Participating in the hearing were Senator Christine Kehoe, Senator Robert Dutton, Assemblymember John Benoit, Assemblymember Betty Karnette and Assemblymember Pedro Nava. Senator Alan Lowenthal was unable to attend the hearing because of a special hearing called in Sacramento.

Attending the hearing were the following officials: Long Beach City Councilmember Val Lerch and Councilmember Bonnie Lowenthal; California Undersecretary of Business, Transportation and Housing, Barry Sedlick; Manhattan Beach City Councilmember Jim Aldinger; Hermosa Beach City Councilmember Michael Keegan; Timothy Lippman, representing Assemblymember Fran Pavley; Samuel Saucedo, representing Senator Nell Soto; Eloy Morales representing Senator Edward Vincent; Deputy Director Michael Dayton, Governor's Office of Homeland Security; Deputy Director Jessica Cummins, Governor's Office of Homeland Security; Paul Lipscomb, Bureau Chief of the Los Angeles Port Police; and Michael S. Bittner, PhD, Dean of Sponsored Projects and Extended Learning for The California Maritime Academy. Assemblymember Jenny Oropeza's Chief of Staff, Sharon Weissman, attended the hearing and read a prepared statement on behalf of the Assemblymember.

Protecting the Nation's Seaports: Balancing Security and Cost

Jon Haveman, Program Director for the Public Policy Institute of California, co-edited "Protecting the Nation's Seaports: Balancing Security and Cost," with Howard J. Shatz, that was released June 28, 2006. Committee members were provided copies of the PPIC report in advance of the hearing, which provided important background information. In their analysis, Haveman and Shatz identify key shortcomings in maritime security efforts today: the failure to include labor groups in port security planning, competing legislation covering the same tasks, reliance on voluntary actions with limited verification and monitoring, and inadequate funding. They recommend general government revenue as the most appropriate source of funding for port security, "with regulatory requirements that the private sector would have to meet and pay for through methods they devise."

The PPIC report detailed the challenges facing today's maritime industry, both at sea and landside. Haveman stressed the importance of planning, funding, staffing, equipping and training for response and recovery phases in addition to preparedness efforts, stating that the vulnerability of goods in transit is best described as, "goods at rest are goods at risk." There are approximately 17 points at which cargo is vulnerable to tampering by terrorists or thieves during the waterborne supply chain.

In 2004, 20 million containers crossed the globe, including empties returning to ports that may not receive the same attention given to full containers. The supply chain is porous.

The traditional response to a terrorist act has been to implement security measures that directly respond to what just occurred, perhaps overreacting to one incident at the risk of not maintaining a broad defense.

Should 55% of activities shut down for one year at the Port of Los Angeles and the Port of Long Beach, the economic impact to the American economy would be $45 billion, equivalent to one-third of 1% of the U.S. economy, and the loss of 280,000 jobs. Two-thirds of the economic loss would be felt outside the state, which demonstrates the important role the ports play in the national economy. The report also shows that such a loss would mean that goods movement would be delayed, but not stopped. The flexibility and robustness of the U.S. economy and implementation of response and recovery plans would impact the net effect.

A special report on port security produced by KCET, which aired on "California Connected" on May 5, 2006, was screened during the hearing. The video provided a visual overview of the size of the Port of Long Beach and Port of Los Angeles, and the challenges involved in providing a comprehensive maritime security strategy for such a large and diverse facility.

How secure are California's ports today?

To determine how secure California's ports are today, the committee called on U.S. Coast Guard Captain Paul Wiedenhoeft, Captain of the Port for the San Pedro Bay Ports; Gary Winuk, Chief Deputy Director of the Governor's Office of Homeland Security; and Cosmo Perrone, Director of Security for the Port of Long Beach, representing the California Association of Port Authorities.

Captain Paul Wiedenhoeft is the Sector Commander of the Coast Guard's 11th District. He believes it is impractical to inspect 100% of cargo vessels and cargo containers because such an approach would impede the flow of commerce, and the costs would be excessive. A layered defense in an established security zone that emphasizes the use of technology and information sharing can provide security to the supply chain.

The Coast Guard works closely with Customs and Border Patrol with the goal of determining that all cargo arriving in American ports is legitimate. The Coast Guard establishes an operational presence in ports based on an adopted plan that involved stakeholders as part of the Area Maritime Security Committee. According to Captain Wiedenhoeft, no single agency can secure a port alone. Ships that haven't called in a port before get extra attention. It takes strong and effective partnerships to implement a comprehensive port security plan. Coast Guard funding has increased since September 11, with significant amounts going towards replacing Coast Guard cutters, communications systems and essential equipment, but it is unlikely that such high funding levels will continue.

Cosmo Perrone, Director of Security for the Port of Long Beach, represented the California Association of Port Authorities (CAPA) at the hearing. According to Perrone, too often security systems look at where terrorists might hide versus allocating funds to know what is inside the cargo containers, trucks and freight cars crisscrossing the country. At present, it is not known where all the containers are at any given time. Of equal concern are the large numbers of empty cargo containers entering American ports from the landside, which are neither inspected nor tracked.

Ports operate as businesses, and according to Perrone it is important that a business impact analysis be done so that a rapid response and recovery strategy can be planned and implemented. Inspecting 100% of all containers would be ideal with an ability to evaluate and inspect cargo containers from the time they enter the country until they are delivered to their destination, but it is not likely given current funding constraints.

According to Perrone, it is important that those responsible for maintaining a secure port randomize their actions, so that patrol routes and times shift and the use of real time surveillance technology be shared with business entities within a port and among port operators.

Gary Winuk, Chief Deputy Director for the Governor's Office of Homeland Security, stated that Governor Schwarzenegger has directed that protection of the state's ports is a priority. The 2006-07 budget allocated $5 million to improve port security and directed that OHS work with local agencies as they write and submit their port security grant applications to increase the amount of federal funding. Work on a statewide master plan is currently underway and is expected to be completed by the end of 2006. Port security funds are included in Proposition 1B, the transportation infrastructure state bond proposal before the voters on November 7, 2006.

According to Winuk, when the cities of San Diego and Sacramento lost their Urban Area Security Initiative (UASI) status, it meant an immediate loss of funding for this year. OHS is working with the two cities to convince the federal Department of Homeland Security that its determination of risk for the two cities was faulty. The state has made restoring the UASI funding a priority.

OHS works closely with the Coast Guard, and together they co-hosted a conference in Sacramento on August 15-17, 2006, entitled "Moving the Safety and Security of California Forward: Transportation Infrastructure & Maritime/Ports Forum."

OHS created a State Terrorism Threat Assessment Center and four Regional Terrorism Threat Assessment Centers in order to facilitate information sharing among agencies. OHS works closely with the California Maritime Academy, the west coast's training facility for maritime workers, and provides specialized training to the students. OHS has established partnerships with other state agencies including the Governor's Office of Emergency Services, California Highway Patrol, and California National Guard. OHS supports the Transportation Worker Identification Credential (TWIC) program, but would like to see it expanded overseas to cover workers in foreign ports.

Transportation Worker Identification Credential (TWIC) Implementation

The TWIC program utilizes a card with a microprocessor that uses a radio frequency to wirelessly transmit to a card reader so that identity and information can be verified. Plans call for the use of a card that would be swiped at an entry point and used with a 6-digit pin number, with the entire process taking no more than four seconds. A TWIC card would be required for all individuals who need unescorted access to secure maritime areas including vessels, terminals and port facilities, and for all U.S. Coast Guard credentialed merchant mariners.

To qualify for a TWIC card, the applicant must provide a full name, any previous names, address, date of birth, and a full set of fingerprints. A background check is conducted, and there are disqualifying criminal offenses that include espionage, treason, murder, kidnapping, rape, bribery, conspiracy, and the like.

Within days after the August 11 hearing, the Transportation Security Administration (TSA) and Coast Guard decided to phase in the TWIC implementation. Port and vessel owners and operators will not be required to purchase or install card readers until a new rule is released. More than 1900 comments were received during the original TWIC comment period and a new comment period for phase two will be announced.

The TWIC program began in 2003, but was recently fast-tracked by the Department of Homeland Security when questions were raised about the potential for foreign operators of American port facilities. It is estimated that 750,000 maritime and port workers will be affected by the initial implementation of the program. Ultimately, about 10 million people would be required to have the cards.

Committee members heard testimony from Mike Mitre, Director of Port Security for the International Longshore and Warehouse Union (ILWU). The ILWU in California, Canada, Mexico, Alaska & Hawaii represents over 25,000 longshoremen, port and dockworkers. He is a crane operator working on the large overhead gantry cranes loading and discharging vessels calling on the Port of Los Angeles and the Port of Long Beach, and is experienced in running both yard and vessel operations.

Mitre testified that he'd like to see 25% to 30% of cargo containers entering American ports inspected, although 100% would be preferred. He predicted that at some time in the future public safety will likely prompt the tracking of goods consistent with what FedEx and UPS do in tracking their shipments.

In an ideal situation, it would be people who understand how terminals operate who design future maritime security systems, because they would understand all aspects of the strategy. According to Mitre, most port workers live close by, so if an incident takes place their families would be in the potential impact zone. Port workers have a vested interest in ensuring that ports are adequately protected.

Although the ILWU fully supports the TWIC biometric recognition program and has since the beginning, it has specific and serious concerns that should be addressed, especially if there are plans to expand its usage to other modes of transportation. Mitre expressed concerns that TWIC is not ready for implementation largely because the TSA wants to use a new biometrics reader that hasn't been prototyped. Also, it is unclear how truckers and workers on cargo vessels will have their backgrounds checked. Many of those working on the vessels are foreign born, and the large number of truckers working for low pay in a high turnover job has made it impossible to generate a master registry of all current truckers.

In the spring of 2006, the ILWU voluntarily submitted a list of the names of all port workers which was vetted by the Coast Guard, according to Mitre. That same form of verifying who is currently working in local ports has not been done for the truckers. Plus, according to Mitre, waving a driver's license at a port entry gate from 4 to 10 feet away isn't an accurate way to check a driver's identification. He cited a recent check where the "same" driver went through the gate 14 times in two days, which isn't likely when the average truck driver brings in two loads per day.

Mitre also expressed concern about a current national policy that the radioactive screener is placed at an exit gate for the port, which means that one or more containers could sit in a port for days before it is checked for its radiation level.

Where are the gaps?

Dr. Larry Mallon is a professor at the California State University at Long Beach. He is coordinating California's first comprehensive port security survey and capability gap analysis as Chair of the AB 2043 CALMITSAC Port Security Study Committee (California Marine and Intermodal Transportation Advisory Committee). In 2004, then-Assemblymember Alan Lowenthal authored AB 2043 which called for a goods movement statewide strategic plan: the "Growth of California Ports: Opportunities and Challenges."

While the report is due to the Legislature in February 2007, Dr. Mallon provided committee members with insights on gaps that have already been indicated during initial responses to the survey. The intent of the study is to develop a strategic plan for a new entity formed by the California State University system: the Port and Intermodal Systems Center for Enhanced Security (PISCES). The founding members are the California Maritime Academy, CSU San Bernardino, CSU Long Beach, CSU Los Angeles, San Diego State University and Cal Poly San Luis Obispo. PISCES was formed in response to a Congressional legislative initiative in the Coast Guard and Marine Transportation Act of 2004 to provide a long term strategic and collaborative approach to address port, intermodal and other transportation-related critical infrastructure, efficient goods movement and national security issues.

According to Dr. Mallon, it is important that as successful port security programs are developed and implemented, that they are shared so that they can be replicated at other sites. An effective port security program looks at the entire goods movement system, tracking everything flowing through ports inland to the ultimate destinations. This can be done in a variety of ways including the installation of road and rail sensors and having the CHP conduct more truck inspections.

With the assistance of the California Maritime Academy, a detailed survey designed to provide a snapshot view of the status of port security in California was hosted on a secure website at the San Diego State University Research Foundation.

Dr. Mallon recommended that federal and state efforts be combined to improve training, certification, exercises and greater collaboration between first responders and port and longshore workers, replicating the Joint Harbor Operations Center (JHOC) structure in use in San Diego.

Captain Ralph Tracy chairs the Security Committee for the American Association of Port Authorities (AAPA). He is the Port Police Commanding Officer of Detectives and Counterterrorism for the Port of Los Angeles. AAPA represents ports in both North and South America. AAPA supports the federal TWIC program but does not support new taxes to pay for it. Enhancing maritime security and protecting America's seaports from terrorist acts is a major priority for AAPA and port authorities.

The federal government decides whether cargo will be allowed to enter the United States. The Coast Guard and Customs and Border Protection determine which ships and which goods can enter, but once the cargo is cleared for entry it is the port authorities and terminal operators that are responsible for moving cargo off the ships, storing it on the port facility and then loading it on trucks or rail so it can be transported to its ultimate destination.

The federal government has just shifted its funding approach to a risk management focus, determining the threat, vulnerability and criticality of the specific infrastructure. At the same time, San Diego and Sacramento lost their federal UASI status; therefore, millions of dollars per year of previously assured funding is lost. A comprehensive maritime security strategy requires adequate funding, which AAPA estimates to be $400 million per year. The ultimate goal is to have a dedicated funding source so that inconsistencies in funding do not hamper implementation of essential programs. According to AAPA, the maritime industry pays billions of dollars in user fees and taxes to the government, including $17.5 billion in Customs duties, and marine cargo constitutes about 70% of the annual fees collected by Customs.

Until January 2006, Noel Cunningham, Principal of The MARSEC Group, served as the Director of Operations and Emergency Management for the Port of Los Angeles. Prior to that he served as both the Director of Operations and the Chief of the Los Angeles Port Police. Cunningham believes security starts with people and determining who is working

in our ports. He recommends investigating the statewide security systems used in New York, New Jersey and Virginia.

Cunningham expressed concern about the lack of integration of security systems at the local, state and federal levels, which means that if a problem is discovered, it is not shared with other ports or agencies and generally stays within that level of government. Funding resources are not adequate to deter, detect, respond, and recover, partly because he believes many times federal grants are distributed based on who writes the best essay, not where the risk is greatest. He recommends including as part of planning requirements that resources match the mission.

With the impending implementation of the TWIC program, Cunningham believes the state must play a major role including close monitoring. This is because the state understands the common problems: the large number of truckers and the CHP's role in investigating problems on the highways and verifying identifications. Creating an integrated security system for the state's ports should set as its highest priority working with the private terminals in the use of cameras. He also stressed the importance of working together and sharing intelligence. For example, if someone trespasses at the Port of Long Beach, and again several months later at the Port of Oakland, it is unlikely that it is a coincidence. That's how real time surveillance and situational awareness assessing movement, behavior and looking for objects left behind can make a difference in the use of cameras.

How has port funding been spent and what's in the future?

Gary Winuk, Chief Deputy Director, Governor's Office of Homeland Security, submitted a written report on behalf of Matthew Bettenhausen, Director of the Governor's Office of Homeland Security, who was unable to attend the hearing due to the evolving situation in England following the discovery by British authorities of a terrorist threat.

Should we fail in protecting our ports, what consequences can we anticipate, and what steps should California ports take now?

Dr. Jim Moore is a Professor of Industrial and Systems Engineering at the University of Southern California's (USC) Center for Risk and Economic Analysis of Terrorism Events (CREATE). He and his fellow collaborators at USC, Dr. Peter Gordon and Dr. Harry W. Richardson, have developed and tested the National Interstate Economic Model (NIEMO) and applied it to simulate the economic impacts of terrorist attacks on any of three major U.S. seaports. It is the first operational model of its sort. In simulating terrorist attacks, the effects on intrastate and interstate goods movement, and how economic sectors would be affected, are detailed. His PowerPoint, which is included at the back of this report, shows the distribution of economic impacts by state should the Port of Los Angeles and Port of Long Beach be shut down for one month.

The predicted impacts on specific sectors, show that a one month shutdown of Los Angeles/Long Beach would result in a $3,997M effect on Electronic and Other Electrical Equipment; for New York/New Jersey a $933M impact; and for Houston a $414M impact. The loss to the Motorized Vehicles (including parts) sector by a one month shutdown of Los Angeles/Long Beach would be $1,779M; for New York/New Jersey $1,117M; and for Houston $241M. Other examples are included in the PowerPoint.

According to Dr. Moore, the ports of Los Angeles and Long Beach are national resources and, as such, it should be the federal government that should be providing the funding for port security – not the state. The Governor and Legislature should work together to maximize the federal funds made available to California's ports, and in doing so, emphasize that risk-based funding should move the state's ports to the highest funding priority category.

One of the challenges is to demonstrate at the national level that maintaining secure ports can directly affect even those states that don't have ports, because the economic effect of the shutdown of one or more major ports would be felt across the country.

Each day, men and women throughout the world load and unload cargo, transport goods across oceans and land, as the global marketplace works to meet human wants and needs. That same industry is imminently vulnerable to attack as transportation systems make the world smaller and smaller. It is the job of the Legislature to ensure that the state does its best to make sure that protections are in place, so that commerce in today's "just-in-time" economy, where goods are manufactured and shipped within days of need, works to meet the needs of the public.

The security of ports and waterways is everyone's responsibility - those who work in the terminals and on the vessels, those who travel on our waterways, transportation workers and government officials.

Public Comment

Members of the public had an opportunity to comment on the day's proceedings. Jim Wilkinson, Facilities Security Manager for HANJIN at the Port of Long Beach, expressed concerns about how labor intensive it is to apply for grants, with no guarantee that a site will be funded. He commented on the Maritime Transportation Security Act of 2002 (MTSA) security planning process in place at ports, with close coordination with the Coast Guard. According to Wilkinson, hazardous materials are inspected by the Coast Guard at one terminal per day. Only two terminals are authorized to have hazardous materials at the Port of Long Beach.

The hearing was adjourned at approximately 5:20 p.m.

Findings

Testimony focused on how secure California's ports are today, what gaps exist, and what role the state should play in a comprehensive maritime security strategy. Based upon the testimony, the following findings can be made:

When it comes to maritime security, the U.S. Coast Guard is in charge, but close coordination with other governmental agencies is critical for successful implementation.

- Testimony was consistent throughout the hearing that the U.S. Coast Guard is the lead agency in all maritime security matters.
- Coast Guard funding has increased since September 11, 2001, because there had been a huge backlog of deferred maintenance and the need to replace ships and equipment. However, local commands understand that the funding is not anticipated to continue long-term.
- The Coast Guard has a close working relationship with the many agencies involved in maritime security including the federal Department of Homeland Security, Customs and Border Protection, the Federal Bureau of Investigation (FBI), the Governor's Office of Homeland Security, the Governor's Office of Emergency Services, the California National Guard, State Terrorism Threat Assessment Center and four Regional Terrorism Threat Assessment Centers and the California Highway Patrol. No single agency can assure the security of our ports; strong and effective partnerships are essential.
- The Coast Guard determines which vessels to board and inspect, and which cargo containers to inspect, on a risk-based decision matrix. The Coast Guard also has the authority to prohibit cargo vessels from entering the harbor because required information as to the cargo, crew and any passengers has not been provided.
- The combination of requiring specific information about cargo vessels, their crew and what they're carrying a minimum of 24 hours prior to arrival in an American port, plus random cargo checks, is part of the layered defense for ports that serves as a deterrent for terrorist action.
- Federal legislation requires that Area Maritime Security Committees be established in states with active ports. The committees, co-chaired by the Coast Guard Port Captain and an FBI official, do long range planning and participate in large scale counterterrorism exercises.

How safe are California's ports today?

- The use of advanced technology surveillance systems has greatly improved detection efforts at large infrastructure sites such as ports where there are multiple points of ingress and egress, multiple transportation modes, bridges, numerous terminals, public docking areas and a large number of recreational boaters, and storage on the landside of large numbers of empty cargo containers.
- The inspection rate for cargo containers averages 5 to 6 percent.
- According to the June 28, 2006, PPIC report, the annual turnover in truck drivers at the ports is approximately 30 percent. An estimated 35,000 cargo truck trips are made each day on the state's freeways.

- Approximately 40% of all containers carry mixed loads from different sources, with different goods going to multiple destinations.
- The traditional response to a terrorist act has been to implement security measures that directly respond to the type of incident that just occurred, perhaps overreacting to one incident at the risk of maintaining a broad defense.
- Too often the security systems in place look at where terrorists might hide versus knowing what is inside the cargo containers and where the trucks and freight cars hauling them are as they crisscross the country, with no tracking system in place.
- The definition of "physical inspection" of a cargo container potentially has many different interpretations: from visually inspecting the interior to installing radiation portals at the exit to a port to actually opening and checking loads as they leave the terminal.
- A national policy calls for radiation portals to be placed at a port's exit. Therefore, a cargo container could sit on port property for days or weeks, emitting harmful radiation, chemical or biological emissions, before it is discovered.
- Ports are not isolated; most often they are located in or near high density residential and industrial areas. Evacuation plans should be coordinated between port officials and local governments.
- While the federal government generally focuses on disaster prevention and preparedness efforts and funds for equipment and training, it may be appropriate for the State of California to take the lead on response and recovery efforts because of the close working relationships at the local government level already in place.
- Port security is consistent with the strategies and approaches incorporated in the California Standardized Emergency Management System (SEMS) and the National Incident Management System (NIMS), which is patterned after SEMS.
- Research conducted by universities and nonprofit private institutions continue to provide insights into current maritime security operations and directions for improvement.
- The Office of Homeland Security established a State Terrorism Threat Assessment Center and four Regional Terrorism Threat Assessment Centers in order to facilitate the sharing of intelligence information and coordinate planning and response efforts.
- An integrated security system involving all ports within the state including the use of cameras and real time exchange of information enhances the state's ability to prevent terrorist attacks and detect suspicious behavior.
- The California Maritime Academy is part of the California State University system, and in conjunction with the Office of Homeland Security, offers training for maritime workers in homeland security techniques, policies and practices.
- The operators of ports and terminals are in direct competition with other port and terminal operators. The ability to share intelligence and surveillance information at individual ports and terminals with other ports and terminals throughout the state improves the ability to detect and perhaps prevent potential terrorist attacks.
- Recreational boaters generally have open access to many of the same areas of a bay or channels leading into a port's terminals.

- Truckers usually average two loads per day, are paid by the individual load, and are subject to long days and low pay. Their vehicles are rarely visually inspected in the cab/sleeper cab areas.

TWIC, alone, will not protect the state's ports from a potential terrorist attack.

- The federal Department of Homeland Security has designated the Transportation Security Administration (TSA) as the agency responsible for designing and implementing the Transportation Worker Identification Credential (TWIC). The challenges in implementing an effective, efficient and successful TWIC program are significant; they include the financial cost to the individual applicant (about $140 each) and the amount of time necessary for the thousands of workers required to be TWIC certified. It is unclear what the state's role is in designing and implementing the TWIC program.
- Within days after the August 11, 2006 hearing, the TSA announced it would go ahead with processing TWIC applications, but hold off on requiring the ports to install the biometrics card readers until a later date.
- Because ports generate a significant amount of traffic congestion, ports have their own "first responders" who maintain the scene until the region's first responders can access the site.
- There are incentives that those in the maritime goods movement might consider, such as offering expedited service if cargo containers, individual shipments, trucks, freight cars, etc., utilize tracking devices or other security measures.

Setting minimum safety standards assists in determining funding strategies. How do we determine how safe is safe?

- Because port workers often live in adjacent communities to the ports, concern over the wellbeing of their families may mean port workers might leave the port in response to an incident.
- It is likely that even minimal operations at a port will not be possible until such time as assurances are in place that minimum safety standards have been re-established following an incident. Establishing minimum safety standards in advance would expedite the decision making on when to re-open.
- If the state's ports have minimum safety standards in place such as for background radiation readings, it is more likely that regulators would know whether "normal" conditions are in effect following an incident.
- Determining minimum standards for the number and type of safety equipment, staffing and training for the state's ports would help in prioritizing grant allocations and discretionary funding.
- Inconsistencies year-to-year in funding for port security initiatives restricts long-term staffing and the purchase and maintenance of essential equipment.

Ports are prime targets, but they may also be subject to collateral damage. Having a business plan in place will assist in good decision making should a disaster strike.

- While the state's ports are considered by terrorist experts to be prime targets, it is possible that ports may not always be the main target. They could suffer collateral damage should bridges, train tracks or highways be damaged, resulting in the disruption of goods movement.
- Appropriate decisions on determining priorities for goods movement are more likely when port authorities have in place continuity of business plans created through stakeholders working together to identify challenges and opportunities in maximizing efficiency and minimizing economic impacts. Who determines which goods should be moved first, and based on what criteria? Regular training opportunities will assist stakeholders in determining what should be involved in the decision, and how priorities would be determined.

Funding continues to be a challenge.

- According to the PPIC report, since September 11, 2001, California ports have received $150 million out of the total $779 million dispensed through the federal Port Security Grant Program, the Urban Areas Security Initiative (UASI), and Operation Safe Harbor. The State of California passed through an additional $5 million in federal funds directly to ports. In 2006, the federal government announced that Sacramento and San Diego were no longer eligible for UASI first tier funding.
- Ports are national resources and the federal government should be the primary funding source for port security measures. It is difficult to convince people in other parts of the country of the essential role California's ports play in their local economy.
- Funding for expanded and enhanced port security is included in Proposition 1B, the Highway Safety, Traffic Reduction, Air Quality, and Port Security Bond Act of 2006, before California voters on November 7, 2006. If passed, it would authorize $3.1 billion for the California Ports Infrastructure, Security, Air Quality Improvement account and $100 million to the Office of Emergency Services for port, harbor and ferry terminal security improvements, out of a total $19.925 billion bond.
- OHS has been working on grant writing with ports and local governments throughout the state to try to increase the likelihood of receiving federal grants. Federal grant proposals are time consuming and complicated to complete, which sometimes deters agencies from applying.
- Following September 11, the New York City Harbor was designated as a "Special Needs Agency" and the result was more federal funding.
- While there is no dedicated federal funding stream for ports, there is one for the nation's airports. The federal government has spent twenty times more on aviation security than on port security since September 11.
- Together the Port of Long Beach and the Port of Los Angeles cover approximately 10,000 acres and about 43 miles of waterfront, and they are identified as the #1 terrorist target in California. The two together are larger than all America's east coast ports combined. There are approximately 15,000 small

craft boats in the area. An average of 12,000 containers per day are unloaded at the two ports.

Security strategies must be able to adapt to shifting priorities and inconsistent funding.

- "Goods at rest are goods at risk." There are approximately 17 points per container at which a cargo shipment is vulnerable to access by thieves and terrorists from its point of origination to its ultimate destination.
- Goods movement capacity at Canadian and Mexican ports varies each day, depending upon where the vessels and containers are at the time an incident occurs. Part of the decision making on whether to divert containers to other ports following an incident is to determine whether there is adequate distribution capacity on the port's landside. Goods must be able to be shipped efficiently on the landside.
- The emphasis on surveillance and inspection at ports is currently focused on full containers coming in to terminals to be unloaded, not on the millions of empty cargo containers returning to ports with little to no inspection or paperwork.
- It is impractical to inspect 100% of the 25,000 containers arriving in the nation's ports each day, because it would impede the flow of commerce and there are significant costs involved. The Coast Guard conducts its inspections using risk-based assessments. Until shippers see the economic benefit of tracking containers to their ultimate destination and/or using road sensors, it is unlikely that the current approach to container inspections will change.

Recommendations

The Governor's Office of Homeland Security should be directed to complete the comprehensive maritime security policy that is currently being drafted, so that a statewide protocol is adopted as soon as possible. Without an adopted statewide strategy, ports, state agencies, and local governments have a difficult time coordinating their efforts to identify and implement steps to improve port security on the landside.

Currently, a "layered defense" is in place that includes intelligence operations, requirements that the type and amount of goods being shipped be reported to the federal government prior to shipping, adopting uniform shipping rules so that it is easier to note variations, limiting access to ports and terminals, and expanding the use of technology.

While the federal government has emphasized prevention, preparedness and detection efforts, the state is uniquely qualified to address response and recovery planning and implementation. Should a natural or human initiated disaster take place within or adjacent to one or more of the state's ports, it would be the state that would respond to restoring basic services including transportation modes. The federal Maritime Infrastructure Recovery Plan was released in April 2006 and provides a framework for federal actions related to ports during the recovery phase, but restoring highways and freight train travel often requires extensive interaction between state and local governments.

The Governor and State Legislature should work closely with the Congressional Delegation to obtain a greater risk-based share of federal port and homeland security funding. Past funding patterns at the federal level favor allocating a disproportionate share of maritime security dollars to east coast ports.

Expanding and Enhancing the State's Role in Port Security

Funding

- Evaluate whether grants of state funds are based on threat, vulnerability and criticality of the proposal.
- Evaluate alternative funding sources.
- Determine appropriate funding levels for equipment and staffing to secure the state's ports. Establish minimum baseline standards for equipment, staffing and training necessary to secure each port to ensure that both technical needs and staffing needs are met.

Research

- Encourage universities and nonprofit private institutions to provide insights into current maritime security operations and directions for improvement, including direct state involvement on the landside.
- Research whether the state should establish basic port police powers to establish security zones on the water in a consistent manner.
- Evaluate ways in which the California Highway Patrol, with its expertise in highway safety and trucker identification, can assist in helping design and implement TWIC.
- Analyze a role that the CHP could play landside on checking empty cargo containers re-entering ports via trucks and freight trains.
- Evaluate the statewide maritime security systems in place in the states of New Jersey, New York and Virginia to determine potential applications in California.
- Evaluate alternatives to the national policy requiring that radiation detection portals be located at port exits to deal with the potential of nuclear, biological or chemical weapons that are designed to detonate in place in cargo containers that never leave a terminal.
- Evaluate available technology that would enable trucks, containers, trains, etc., to be tracked as to their location from their point of origin to their final destination using real time monitoring and reporting.
- Research ways in which recreational boaters can become additional "eyes and ears" in efforts to improve maritime security, that might include the Community Emergency Response Team (CERT) model, Retired Senior Volunteer Patrol (RSVP) programs, etc.
- Develop a recovery strategy that includes having the maritime industry at the table so that, in restoring the system following an incident, government does not

make the decisions alone on when and where goods are moved back into the system.

- Research methods by which radiation detectors can be used safely both on land and at sea.

Planning

- Participate in the planning for, and implementation of, the TWIC biometric card reading program.
- Encourage development of emergency response capacity within the state.
- Incorporate response and recovery strategies into statewide maritime plans, and require port operators to adopt continuity of business plans as part of their response and recovery planning.
- Encourage more coordination of grant requests among port operators.
- Ensure that evacuation plans adopted for the state's ports are coordinated with those of neighboring communities, and updated on a regular basis. Determine when it is necessary to evacuate an entire port, and when only a designated area needs to be evacuated. Determine who must shelter in place and who must evacuate.
- Work with labor unions, first responders and other stakeholders to establish minimum safety standards that would have to be met before workers return to a port following a catastrophic event.
- Study alternative sites that may be used for loading and unloading goods should a port shut down, along with any other actions that might be necessary, such as dredging, additional highway lanes, train track upgrades, etc., that should be done in advance of need.
- Establish minimum training standards for port workers utilizing the CERT model so that they can respond in an emergency and assist first responders.
- Establish minimum security training for port workers comparable to that offered to private security officers by OHS so they can serve as additional "eyes and ears" for potential security breeches. Involve port workers in annual training exercises.

Statewide Coordination

- Encourage the ability of port operators and terminal operators to share real time intelligence and surveillance information with other ports and terminals throughout the state in order to improve the ability to detect and prevent terrorist attacks.
- Encourage combined federal and state efforts to improve training, certification, exercise and greater collaboration between first responders and port and longshore workers, replicating the Joint Harbor Operations Committee (JHOC) structure in use in San Diego.
- With input from the maritime industry, develop a recovery strategy so that governmental entities alone do not make decisions on when and where goods are moved back into the system after an incident.

Jon Haveman, Program Director, Public Policy Institute of California, Editor, "Protecting the Nation's Seaports: Balancing Security and Cost," issued June 28, 2006.

Jon D. Haveman is a research fellow and director of the Economy program at the Public Policy Institute of California. He is a specialist in the effects of international barriers to trade, international competition policy, and transportation and security issues as they pertain to servicing internationally traded goods. He is the author of Institute reports entitled *Protecting the Nation's Seaports: Balancing Security and Cost* and *California's Global Gateways: Trends and Issues* and more than 25 published articles in the area of international trade. These articles include *The Benefits of Market Opening, The Determinants of Long Term Growth,* and *The Effects of U.S. Trade Laws on Poverty in America.* He was previously on the faculty in the Economics Department at Purdue University, has served as the Senior International Economist at the President's Council of Economic Advisers, and has been a visiting fellow at the United States Bureau of the Census. He has also worked as a research economist at the Bureau of Economics at the United States Federal Trade Commission. He holds a B.A. in economics from the University of Wisconsin, Madison and an M.S. and Ph.D. in economics from the University of Michigan, Ann Arbor.

CAPTAIN PAUL E. WIEDENHOEFT, USCG
BIO

Captain Wiedenhoeft is the Commander, Captain of the Port, and Federal Maritime Security Coordinator for the U.S. Coast Guard's Sector Los Angeles-Long Beach. From offices on Terminal Island in San Pedro, Sector Los Angeles-Long Beach operations include an area of responsibility that stretches approximately 320 miles along the California coast from north of Morro Bay down to the San Diego County line. Within this area, the Sector is directly responsible for port safety and security, maritime law enforcement, search and rescue, and shoreside aids to navigation. This area of responsibility includes the Los Angeles-Long Beach port complex, as well as Port Hueneme.

During his Coast Guard career, Captain Wiedenhoeft has sailed in five Coast Guard cutters, commanding a patrol boat, a buoy tender, and a medium endurance cutter while conducting all Coast Guard missions afloat from the waters of Southeast United States, the Caribbean Sea, Western and North Pacific Ocean, and to the Bering Sea and Arctic Circle.

Ashore, Captain Wiedenhoeft has served as a Rescue Coordination Center Controller and District Command Center Watch Officer in Seattle, Washington and in two different offices at Coast Guard Headquarters in Washington, DC with emphases in senior-level management effectiveness and enterprise logistics information.

A native of Beaver Dam, Wisconsin, he received his commission in 1983 from the Coast Guard Academy. Captain Wiedenhoeft holds a Master of Science degree in Information Technology Management from the Naval Postgraduate School in Monterey, California and a Bachelor of Science degree in Electrical Engineering from the Coast Guard Academy. His personal awards include a Meritorious Service Medal, multiple Coast Guard Commendation Medals, and a Coast Guard Achievement Medal.

* * * *

Pronunciation: Wee'-den- heft

OFFICE OF HOMELAND SECURITY

Matthew R. Bettenhausen
Biography

Matthew R. Bettenhausen was appointed on March 24, 2005 to serve as the Homeland Security Advisor to Governor Arnold Schwarzenegger and the Director of the California Office of Homeland Security.

Prior to his appointment in California, Matt served as the first Director of State and Territorial Coordination with the U.S. Department of Homeland Security. There, Matt was responsible for coordinating the efforts of the Department as they relate to state, territorial and tribal governments. He served on White House Senior Policy Coordinating Committees and working groups concerning Homeland Security issues, including work on implementing Homeland Security Presidential Directives. He was also a member of the Department's Emergency Response Group (ERG) and the Interagency Incident Management Group (IIMG).

From January 2000 to January 2003, Matt served as the Deputy Governor of Illinois and its Homeland Security Director. As Deputy Governor, Matt was responsible for coordinating the law enforcement and public safety functions and agencies of the State of Illinois. The agencies reporting to him included among others: the Illinois State Police, the Department of Corrections, Fire Marshal's Office, Illinois Emergency Management Agency, Department of Nuclear Safety and the Department of Military Affairs.

Matt also served twelve years as a federal prosecutor for the U.S. Department of Justice. He investigated and prosecuted all manner of federal offenses from drug cases to complex financial fraud matters and long-term undercover investigations. He held various supervisory positions with the U.S. Attorney's Office in Chicago, including Chief of Appeals and Associate Chief of the entire criminal division. Matt graduated Summa Cum Laude from the University of Illinois with a B.S. in Accountancy. Matt continued his education at the University's Law School and received his law degree with honors.

Matt's family has a long and extensive history in the fire service and law enforcement. His father has spent 50 years in the fire service and currently is the Fire Marshal for Tinley Park, Illinois. His brother is an officer with the Lemont Fire Protection District.

GOVERNOR ARNOLD SCHWARZENEGGER • DIRECTOR MATT BETTENHAUSEN
OFFICE OF THE GOVERNOR, SACRAMENTO, CALIFORNIA 95814
(916) 324-8908 • FAX (916) 323-9633

BIOGRAPHY

COSMO PERRONE

DIRECTOR OF SECURITY

Cosmo Perrone, with more than three decades in the security field, is the Port of Long Beach's Director of Security. The Board of Harbor Commissioners appointed the former Boeing and McDonnell Douglas Security and Fire Director to his position at the Port in March 2005.

Heading the Port's Security Division, Perrone oversees more than 50 security personnel and directs the Homeland Security, Emergency Management and Business Continuity, and Harbor Patrol functions which provide security coverage for the 3,000-acre Port complex.

Perrone was previously the Executive Director of Cosmo Perrone and Associates of Long Beach, a security, fire and emergency management consulting firm formed in 2003. Among its assignments, his company helped develop a Maritime Security Plan for a firm located at the Port of Long Beach. He was selected to act as a Physical Security consultant for the National Academies, Science and Technology Committee on the Yucca Mountain Nuclear Waste Site Project.

Prior to that, he served for 23 years in Long Beach with aircraft manufacturer Boeing and McDonnell Douglas (which Boeing acquired in 1997), including 19 years as Director of Security and Fire Services. He was responsible for the development and administration of strategic policy of the company's global security and fire protection functions. He was Boeing's Southern California Executive Coordinator for all Homeland Security issues.

He has been a member of the American Association of Port Authorities, the International Association of Airports and Seaports Police, the American Society for Industrial Security, and the U.S. State Department's Overseas Security Advisory Council. His other memberships have included the California Bar Association, the Aerospace Industries Association, RSA (Research Security Administrators) and he has served on the City of Long Beach Public Safety Commission.

Perrone, a resident of Long Beach, holds Bachelor of Arts degree from Northeastern University in Boston, MA, and a law degree from Western State University in Fullerton, CA.

BIOGRAPHY
MIKE MITRE – BIO
ILWU Director of Port Security

Mike Mitre currently serves as Director of Port Security for the ILWU, and is a working member of Local 13 – ILWU in Southern California. He is a regular crane operator operating the large overhead gantry cranes loading and discharging vessels calling on the Ports of LA and Long Beach. He also is a certified supervisory foreman, experienced in running both yard and vessel operations.

Well-versed in marine terminal and port operations, Mr. Mitre began his multi-faceted career in 1974 working aboard tugboats, barges and the Catalina Island Ferries. Throughout the seventies Mitre worked aboard various tugboats, barges, and other vessels engaged in many different types of work, one of which was carrying passengers to and from Catalina Island. Mitre sat for and was awarded a US Coast Guard Masters License in 1979, thereafter working as a Captain for the Catalina Island Cruise Co. He obtained a casual longshore permit in 1976, and worked as an extra. Mr. Mitre was registered as a full time longshoreman in Local 13 in 1985.

Throughout his years on the waterfront Mitre has served in many positions; among them President of Local 13, the largest longshore local in the country. Mike Mitre currently sits on the ILWU's International Executive Board and represents Southern California's longshoremen, guards, office clerical's, and warehouse workers.

Mr. Mitre was raised in San Pedro and graduated from San Pedro High School in 1972. He attended Cal. State University at Long Beach where he earned his Bachelor's Degree. Mitre has been deeply involved with many levels of port security, infrastructure, and congestion. In 2000, along with Peter Peyton of ILWU Local 63, he co-authored "Seven Problems/Seven Solutions" unveiled at the CITT Long Beach Town Hall Meeting. Mitre was one of the first to formally recognize the need for 24 hour operations and night gates, reducing on-terminal chassis storage and leasing, and maximizing terminal space through more effectively planned "grounded" vs. "wheeled" operations.

Mike Mitre is one of the pioneers of port security within the marine container terminal environment, including the need to employ "best practice" solutions surrounding access control, empty container verification, container seal inspection, etc. Mitre has testified in Washington DC before both Houses of Congress involving port security and infrastructure, including the recent Dubai hearings.

Dr. Larry Mallon has compiled an enviable record of achievement and national recognition as naval officer, admiralty and maritime attorney, transportation and logistics consultant, educator, administrator, and interdisciplinary academic researcher spanning thirty-five years. A 1967 graduate of Georgetown University, he holds advanced degrees from Emory University and the University of Miami. He was the recipient of a first-ever post-doctoral fellowship at MIT-WHOI in Marine Law and Policy.

While enrolled at Emory University School of Law, he was appointed the first-ever Governor's Intern by then Governor Jimmy Carter and was assigned to assist in restructuring the Georgia Department of Corrections. He was also a first-ever appointed intern by the Georgia District Attorneys Association and tried criminal cases while still a law student under a special act of the Georgia legislature. He was the Founder of the Moot Court Society, its first President, and was recognized by the National Order of the Coif and the Order of Barristers for distinguished achievements in appellate advocacy.

He is a veteran of combat duty in Vietnam and fifteen years naval reserve service, including Legal Advisor to the Oceanographer of the Navy. Designated a Proctor in Admiralty in 1978, he is licensed to practice law in the states of California, New York, the District of Columbia and Georgia, and before the United States Supreme Court and every court of special jurisdiction within the Federal judiciary.

He served as the Maritime Counsel to the United States House of Representatives for eleven years. He is the principal author of the Water Resources Development Act of 1986 (Public Law 99-662), the primary organic law of Federal navigation project development, in addition to numerous statutes codified in Titles 14 Coast Guard, 33 Navigation and 46 Shipping to the United States Code. He was a Congressionally appointed Official Observer to the Third United Nations Conference on the Law of the Sea serving on the staff of then U.S. Ambassador Elliot Richardson (and the author of Marine Environmental provisions in the final draft treaty), and member of the U.S. delegation to the International Maritime Organization's Marine Safety and Legal Committees. He was the founding staff director to the 230 member Congressional Port Caucus in the House of Representatives.

He also served as Legal Consultant to the California State Senate Select Committee on the Maritime Industry, and is the author of an entire body of law involving innovative transportation infrastructure financing codified in the Harbors and Navigation Code. He is a nationally recognized expert in water resources infrastructure development and public financing representing cities, counties and special districts throughout the State of California since 1987 in that capacity. He serves as Counsel to the California Maritime Infrastructure Authority. He is the Founding Chair of the Southern California Marine Transportation System Advisory Council to the Secretary of Transportation. He sits as a national representative on the Legal Committee of the American Association of Port Authorities.

He served as founding Director of Research and Counsel to the Center for International Trade and Transportation at California State University Long Beach, a nationally designated center for goods movement research by the Secretary of Transportation. He is currently engaged in applied research for the Departments of Defense, Transportation and Homeland Research in freight movement and intelligent transportation systems, maritime, port, and global supply chain security, and rapid deployment, warfighter sustainment and force protection.

CAPTAIN RALPH L. TRACY
Commanding Officer of Operations

Captain Ralph L. Tracy is the Port Police commanding officer of Detective and Counterterrorism operations for the Port of Los Angeles, one of the largest, busiest and most successful seaports in the nation.

Tracy, who was appointed to his current position in February 2005, manages the Port Police, the only U.S. police force dedicated exclusively to port activities. In this position, he oversees the enforcement of all federal, state and local laws applicable to Port responsibilities, including cargo protection, pollution investigation, vessel traffic control, counterterrorism, and narcotics interdiction.

A 20-year City employee, Tracy has spent the majority of his career as a Port Police officer. After a two-year stint as prosecutor for the City Attorney's Office, he returned to his career in law enforcement at the Port.

A graduate of the FBI National Academy and California Command College, Tracy holds a juris doctor from Western State College of Law. He also served four years in the U.S. army.

Tracy is a member of the American Association of Port Authorities and currently serves as chairperson of the organization's security committee and has done so since 2001. In 1998, the Port of Los Angeles named him "Officer of the Year."

# # #

Marsec Government Services, LLC

Cunningham & Associates, LLC

Firm Principal Biographies

Noel K. Cunningham

Mr. Cunningham is a principal of The MARSEC Group and President of Cunningham and Associates. Until January 2006 he served as the Director of Operations and Emergency Management for the Port of Los Angeles, the busiest and most successful commercial seaport in the nation. Prior to this appointment, Mr. Cunningham served jointly as Director of Operations and Chief of the Los Angeles Port Police (LAPP) – a position he held for 14 years since joining the Port in January 1991. Among his responsibilities, Mr. Cunningham managed the Port Police, Port Pilots, Emergency Preparedness and Homeland Security divisions.

The Port of Los Angeles has the only U.S. police force dedicated exclusively to port activities, while enforcing all federal, state and local laws applicable to Port responsibilities, including cargo protection, pollution investigation, vessel traffic control and narcotics interdiction. The Pilot Services Division makes approximately 5,500 vessel moves a year with a stellar safety record, second to none in the maritime industry.

Before joining the Port, Mr. Cunningham served as an area captain with the Los Angeles Police Department (LAPD), where he completed 25 years of service. Mr. Cunningham is the only twice-honored recipient of the Professional Image Award, LAPD's highest management award.

Mr. Cunningham was one of the organizers of the innovative Sea Marshal Program, a joint effort between the Port of Los Angeles and U.S. Coast Guard to facilitate the flow of vessel traffic during periods of heightened alert by deploying armed officers to protect and secure cruise passengers and high-risk cargo. He also developed the first U.S. cruise ship passenger security plan, which has since been adopted as a national and international model by both the U.S. Coast Guard and International Maritime Organization. Mr. Cunningham has also served as director of the federally-legislated, post-9/11 Operation Safe Commerce program.

Mr. Cunningham is an international renowned port security expert having served as Past President of the International Association of Airport and Seaport Police. He has participated in the Organization of American States Security Panel in the development of improved security practices for ports in South and Central America and the Caribbean. Mr. Cunningham was featured on the cover of the June 11, 2005 issue of the *National Journal* for his security efforts at the Port of Los Angeles.

Mr. Cunningham holds a Master's Degree in Public Communications from Pepperdine University and a Bachelor's Degree in Political Science/Public Administration from California State Polytechnic University, Pomona

The MARSEC Group
200 Pine Avenue, Suite 300, Long Beach, CA 90802
Phone: (562) 435-3825, Fax: (562) 435-5735
Marsecgroup.com

PROFESSOR JAMES E. MOORE II

Curriculum Vitae

Jim Moore is a Professor of Industrial and Systems Engineering; Public Policy and Management; and Civil Engineering at the University of Southern California He is Director of the Transportation Engineering program, Co-Director of the Construction Management Program, and Chair of the Daniel J. Epstein Department of Industrial and Systems Engineering in USC's Viterbi School of Engineering. In 2003, he was elected to the Russian Academy of Natural Sciences, United States Section, for outstanding contributions to the field of Transportation Systems Engineering; and received the Kapitsa Gold Medal of Honor.

Prof. Moore's research interests include risk management of infrastructure networks subject to natural hazards and terrorist threats; economic impact modeling; transportation network performance and control; large scale computational models of metropolitan land use/transport systems, especially in California; evaluation of new technologies; and infrastructure investment and pricing policies. He specializes in transportation engineering, transportation systems, and other infrastructure systems.

Prof. Moore received his BS degrees in Industrial Engineering and Urban Planning in 1981 from Northwestern University's Technological Institute (now the McCormick School of Engineering and Applied Science) in Evanston, Illinois. He received his MS degree in Industrial Engineering from Stanford University in 1982, his Master of Urban and Regional Planning degree from Northwestern in 1983, and his Ph.D. degree in Civil Engineering (Infrastructure Planning and Management) from Stanford in 1986.

RECENT RESEARCH AND SCHOLARSHIP

The Economic Costs and Consequences of Terrorist Attacks, Harry W. Richardson, Peter Gordon, and James E. Moore, II (eds.) Edward Elgar Publishing: Cheltenham, 2006.

The Economic Impacts of Terrorist Attacks, Harry W. Richardson, Peter Gordon, and James E. Moore, II (eds.) Edward Elgar Publishing:

Cheltenham, 2005.

(third author, with Peter Gordon, Soojung Kim, Jiyoung Park, and Harry W. Richardson) "The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System," submitted to *Risk Analysis, An International Journal*, for inclusion in a special issue of volume 26 (2006).

(third and principal author, with Nobuhiko Shiraki, Masanobu Shinozuka, Stephanie E. Chang, Hiroyuki Kameda, and Satoshi Tanaka) "Transportation System Risk Curves: Probabilistic Performance Scenarios for Highway Networks Subject to Earthquake Damage," forthcoming in the *American Society of Civil Engineers Journal of Infrastructure Systems*, **12** (2006).

(first author, with Richard G. Little, Sungbin Cho, and Shin Lee) "Using Regional Economic Models to Estimate the Costs of Infrastructure Failures: The Cost of a Limited Interruption in Electric Power in the Los Angeles Region," *Public Works Management and Policy*, **10**, 3 (2006): 256-274.

(first and principal author, with Michael McNally, Steve Mattingly, and C. Arthur McCarley) "Technical Evaluation of the Anaheim Adaptive Control Field Operational Test: Institutional and Technical Issues," forthcoming in the *Journal of Transportation Planning and Technology*, **28**, 6 (2005): 465-482.

(third author, with Yueyue Fan and Robert Kalaba) "Arriving on Time," *Journal of Optimization Theory and Applications*, **127**, 3 (2005): 1-17.

(third author, with Yueyue Fan and Robert Kalaba) "Shortest Paths in Stochastic Networks with Correlated Link Costs," *Computers and Mathematics with Applications*, **49** (2005): 1549-1564.

(third and principal author, with Donghwan An, Peter Gordon, and Harry Richardson) "Regional Economic Models for Performance Based Earthquake Engineering," *American Society of Civil Engineers / Natural Hazards Research Applications and Information Center Natural Hazards Review*, **5**, 4 (2004): 188-194.

(first and principal author, with John Kuprenas, Jiin-Jen Lee, Peter Gordon, and Harry W. Richardson) "Cost Analysis Methodology for Advanced Treatment of Stormwater: The Los Angeles Case," *Journal of Construction Research*, **5**, 2 (2004): 1-22.

(first and principal author with Genevieve Giuliano and Seongkil Cho) "Secondary Accident Rates on Los Angeles Freeways," *American Society of Civil Engineers Journal of Transportation Engineering*, **130**, 3 (2004): 280-285.

(first and principal author, with Genevieve Giuliano and Jeremy March) "Field Operational Test Performance of Automatic Passenger Counters," *Intelligent Transportation Systems Journal*, 7, 2 (2002): 131-150.

(first and principal author, with Seongkil Cho and Daniel Mezger) "Feasibility of Using Los Angeles Freeway Service Patrol Trucks as Probe Vehicles," *American Society of Civil Engineers Journal of Transportation Engineering*, **128** (2002): 528-536.

(principal author, with C.Arthur MacCarley, Stephen P. Mattingly, Michael G. McNally, and Daniel Mezger, "Lessons Learned from the Irvine Integrated Freeway Ramp Metering / Arterial Adaptive Signal Control Field Operational Test," *Transportation Research Record*, **1811** Advanced Traffic Management Systems for Freeways and Traffic Signal Systems (Highway Operations, Capacity, and Traffic Control, 2002): 76-83.

(second author, with Myung-Jin Jun) "The Lowry Model Revisited: Incorporating a Multizonal Input-Output Model into an Urban Land Use Allocation Model," *Review of Urban and Regional Development Studies*, **14**, 1 (2002): 1-17.

(second and co-author, with Genevieve Giuliano and J. Golob) "Advanced Technology and Integrated Public Transit: The San Gabriel Valley Smart Shuttle Field Operational Test," *Transportation Research Record*, **1774** Artificial Intelligence and Intelligent Transportation Systems (2001): 44-51.

JUST THE FACTS

SECURING PORTS AND SHIPPING

June 2006

- **An enormous volume of goods flows through U.S. seaports.**
  In 2004, about 1.4 billion tons of freight flowed through 361 U.S. cargo ports. Much of it was shipped inside 20 million ocean cargo containers processed each year at container terminals. Goods in containers account for 59.3% of the total value of all U.S. maritime trade and 14.9% of its total volume. Accordingly, container trade receives the bulk of the attention in debates about port security.

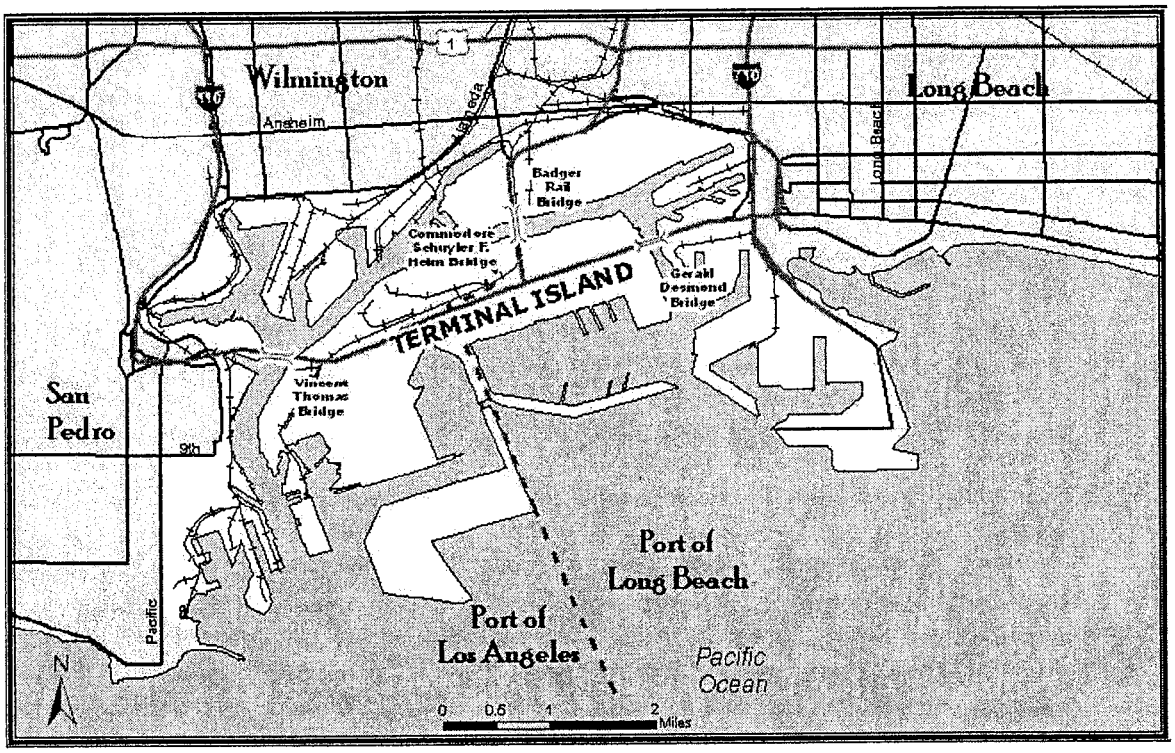
- **Combined, California's largest ports form the 5th largest container facility in the world.**
  The adjacent ports of Los Angeles and Long Beach (see map) are located on San Pedro Bay. Together, they processed more than 7.2 million containers in 2005. More than half of these went through Terminal Island, which has limited access and is therefore more vulnerable to a terrorist attack. The economic cost of such an attack on Terminal Island could total more than $40 billion in the first year. It is unlikely, however, that such an attack would have national economic repercussions.

- **About 70 percent of all containers unloaded in California arrive under provisions of the Container Security Initiative.**
  CSI is a federal program that formally enlists the help of foreign ports in screening containers that are destined for the United States. Currently, 42 foreign ports participate in CSI. More than 70 percent of containers unloaded in California arrive from these ports, about 6 percent of more than 750 ports worldwide that ship containers to California.

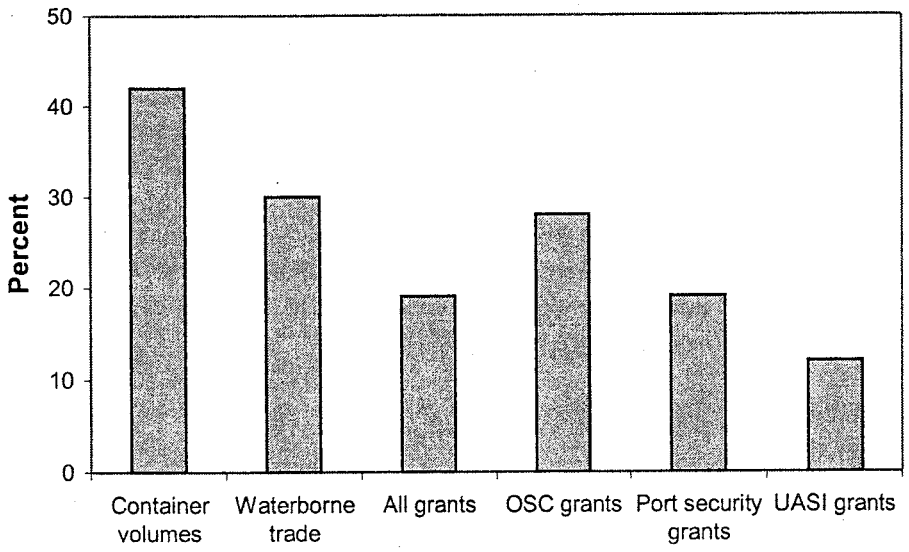
- **Developing security and response strategies at the San Pedro Bay port complex requires coordination among 15 separate government agencies.**
  These include nine at the federal level, among them the Coast Guard, Customs and Border Protection, Immigration and Customs Enforcement, and the Transportation Security Administration; the California Highway Patrol and California Lands Commission at the state level; and local agencies such as the Los Angeles County sheriff's and fire departments, Los Angeles city police and fire departments, City of Long Beach police and fire departments, the Los Angeles Port Police Department and Long Beach Harbor Patrol.

- **California's ports have received significant funding for security through federal grant programs.**
  The federal government has helped finance port security improvements through a grant program, but California's share of these grants is far below its share of containerized trade, or even overall maritime trade. In the years since September 11, California ports have received $150 million out of $779 million in total grants through three programs—the Port Security Grant Program, the Urban Areas Security Initiative, and Operation Safe Commerce. California ports received an additional $5 million of federal money passed through a state grant program.

Los Angeles/Long Beach Port Complex



California's Share of Trade and of Federal Security Grants



RESEARCH BRIEF
Public Policy Institute of California
JUNE 2006 ISSUE #108

Securing the Nation's Seaports: Multiple Goals, Uncertain Results

The recent controversy over foreign management of cargo terminals at six U.S. seaports highlighted just how sensitive and problematic the issue of U.S. port security remains, more than four years after the September 11 terrorist attacks. The nation's 361 ports are seen by most security experts as attractive targets for a terrorist attack because they are so vital to the country's economy: About $807 billion worth of goods passed through American seaports in 2003, 41 percent of all U.S. international trade. Moreover, millions of American paychecks depend on the efficient and secure flow of manufactured goods into U.S. ports from an increasingly global economy. Even before September 11, federal legislators and executives had begun contemplating myriad new programs, many of which they quickly implemented afterwards. But the process remains largely still under construction.

A new report from the Public Policy Institute of California, *Protecting the Nation's Seaports: Balancing Security and Cost*, examines in detail the full dimensions of the task of port security, the effectiveness of measures undertaken so far, and the costs to the nation—both of implementing adequate port security and of failing to do so. Economists Jon D. Haveman and Howard J. Shatz of PPIC teamed with an array of additional experts to marshal a broad overview of port security issues, to examine progress made since September 11, and to suggest how that progress might best be continued. The resulting compilation is a comprehensive assessment. It includes projections of the effects on the national economy of a successful port attack, the private-sector implications of improving port security, a first-hand account of the considerable bureaucratic challenges that still must be overcome at the level of individual ports, and guidelines for financing port security efforts.

Among the highlights:

- Shipping containers are a key vulnerability in the global maritime supply chain system. Containers, the vast majority of which remain uninspected, can serve terrorists in several different ways, and myriad loopholes in global regulations make the container system easily exploitable.
- The creation of comprehensive port attack recovery plans could do much to mitigate the effects of a port terrorist attack, through the reduction of post-attack economic panic and the quick restoration of global supply chains.
- Federal officials should reconsider the adequacy of current port security funding and staffing levels. These have not kept pace with the plethora of new, but often conflicting, programs and initiatives created in the wake of the September 11 attacks.

According to the report's authors, "Better policy guidance is needed. The U.S. government has demanded the implementation of multiple programs simultaneously, without setting priorities."

> *From a politician's point of view, port security emergency response planning is the worst of all worlds: it requires extremely high up-front costs for benefits that will be realized only in the future—most likely when the official is already out of office, and maybe never.*
>
> — from Chapter 6

Possible Economic Consequences of a Port Attack

Predictions about the financial costs to the nation of terrorist attacks on the United States can and do vary wildly in the popular imagination. In this report, two teams of researchers bring some realism to this question. Through different methods, the two teams create a range of possible economic consequences of a hypothetical attack on a major American port, such as Los Angeles–Long Beach. Combined, that port complex processed about $243 billion worth of goods in 2004, or about 10 percent of all U.S. trade; its disruption could have national economic effects.

Edward E. Leamer and Christopher Thornberg of the UCLA Anderson Forecast contend in their analysis that these effects would not be nearly as dire as common wisdom might

assume. Using historical data, they compare a port closure caused by a terrorist attack to similar port closures throughout the country's history caused by labor disputes. During such closures, they argue, the economy was able to bounce back relatively quickly from the reduction in the flow of goods through the ports, even from unexpected shutdowns caused by wildcat strikes. Leamer and Thornberg note further that even the attacks of September 11, although creating a deep national psychological shock and hurting certain industrial sectors, did not result in long-lasting economic damage.

Authors Peter Gordon, James Moore, II, and Harry W. Richardson of the University of Southern California and Qisheng Pan of Texas Southern University argue that the effects of an attack on the Los Angeles–Long Beach port complex, especially one involving radiological weapons, could be very costly. The authors hypothesize a simultaneous attack that isolates Terminal Island, through which more than half of all Los Angeles–Long Beach trade flows. They estimate that a shutdown lasting a year could cause as much as $45 billion in national economic damage, including direct costs, indirect costs, and induced costs—those resulting from reductions in spending by families of employees in affected industries.

Practices and Vulnerabilities

Containers, which revolutionized global maritime trade, draw the attention of two security experts from the University of California at Berkeley. In his chapter, Stephen S. Cohen analyzes the circuitous global journeys of the containers, more than 10 million of which arrive here every year. The threats they pose to security are numerous, Cohen finds, because of the physical impossibility of inspecting all of them, their critical position within just-in-time production systems, and difficulties in tracking them outside U.S. borders. Cohen suggests that a layered defense using multiple technologies, including radiation detectors, may provide the optimal, if expensive, defense.

Jay Stowsky examines the technologies of maritime security and container security in detail—specifically, how government can best encourage the private sector to further develop tools for container surveillance, tracking, and screening. Maritime dual-use technology development should follow a more flexible model than past dual-use practices, Stowsky argues, when large, government-funded systems had limited outside applicability. In the current environment, where wide adoption of common security technologies by players in a globally dispersed sector is the objective, the government would do better to encourage independent research and development and faster, more efficient procurement practices.

Providing security in a large and complex port operation such as Los Angeles–Long Beach, the fifth-busiest container operation in the world, is made especially difficult by the multiple layers of bureaucracies with responsibility for some aspect of port operations and security, according to another of the report's research teams. Amy B. Zegart of the University of California at Los Angeles and Matthew C. Hipp and Seth K. Jacobson of the Riordan Institute for Urban Homeland Security personally worked over a period of years with the 15 agencies from five political jurisdictions that have port responsibility, to improve emergency response to a port incident. Their chapter details just how and why that was and remains such an arduous undertaking. In addition, politics can severely hinder port security efforts, the team found.

Programs and Costs

Editors Haveman and Shatz provide two in-depth analyses of the current state of maritime security, one detailing the responsibility and operations of the multiplicity of current federal programs now in place and the second analyzing how the nation attempts to pay for all of them. Four major programs covering responsibilities including ship and port security plans, container security, overseas ports, and grants for individual jurisdictions now regulate one or more aspects of the problem. Among the initial shortcomings of these, the authors find, were the failure to include labor groups in port security planning, competing legislation covering the same tasks, reliance on voluntary actions with limited verification and monitoring, and inadequate funding. In their analysis of costs, the authors find that the private and public sectors each have an important role in bearing the total cost of port security, which will likely be in the tens of billions of dollars. However, the proper balance between private and public costs remains an unresolved issue. Among the payment sources that have been suggested are user fees, diversion of customs revenues, and general government revenues. The best source of public funds is general government revenue, the authors conclude, with regulatory requirements that the private sector would have to meet and pay for through methods they devise.

This research brief summarizes a report edited by Jon Haveman and Howard Shatz, Protecting the Nation's Seaports: Balancing Security and Cost *(2006, 296 pp. $25.00, ISBN 1-58213-120-1). The report may be ordered online at www.ppic.org or by phone at (800) 232-5343 or (415) 291-4400 [outside mainland U.S.]. A copy of the full text is also available at www.ppic.org. The Public Policy Institute of California is a private, nonprofit organization dedicated to independent, objective, nonpartisan research on economic, social, and political issues affecting California.*

PUBLIC POLICY INSTITUTE OF CALIFORNIA
500 Washington Street, Suite 800 • San Francisco, California 94111
Telephone: (415) 291-4400 • Fax: (415) 291-4401
info@ppic.org www.ppic.org

MICHAEL MITRE – Director of Port Security
INTERNATIONAL LONGSHORE and WAREHOUSE UNION
ON THE
"TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL"
Also known as T.W.I.C.

June 11, 2006

The ILWU represents over 25,000 longshoremen, port, and dockworkers in and around nearly every port on the West Coast, including Alaska and Hawaii. Along with TSA, Homeland Security, and the Dept. of Transportation the ILWU has been involved in the TWIC process from the beginning. While we are fully supportive of any action to improve US port security, the ILWU has grave concerns regarding TWIC, and the flaws that may render it less that adequate. Understanding that there is interest in eventually extending the TWIC program to other modes of transportation adds even more importance that the TWIC program be done properly the first time. Thank for the opportunity to share our concerns.

ILWU port and dockworkers are on the front lines, we're the predominent workforce in ports on the West Coast and as such have a vested interest no else does. Should something happen, it will be ILWU fathers, mother, and brothers and sisters who may not be coming home. Because the majority of our families live within such close proximity of the ports, they stand to be primarily impacted should an attack be carried out against the seaport transportation system.

Access control procedures, including the use of tamper resistant identification cards, new systems technology and biometrics are a major part of the initiatives to identify individuals who pose a real terrorism security risk. Things like barring them from working in transportation jobs now deemed security-sensitive must is a dangerous precedent,and must be dome only in the most extreme circumstances.

It is critical that the TWIC program strike the right balance – it must enhance the security of our transportation system while preserving the legitimate rights of workers; all the time while without unduly infringing on the flow of commerce. The TWIC must provide workers with basic due process rights, including a meaningful waiver and appeal. And it must ensure that privacy rights are respected, and that the focus of the TWIC remains on identifying true security risks, as identified in MTSA Section 70105 terrorism-specific language. TWIC specifically should NOT be allowed to unjustly punish an employee for a bad decision made years ago. In other words, "if we're going to take away someone's job, we'd better be damn sure it's justified and for the right reason."

The ILWU would like to acknowledge the drafting of the Section 70105 language of the Maritime Transportation Security Act (MTSA,) as it establishes requirements and limits for the "job exclusion" process included in the TWIC. The protections and limitations included in this provision are critically important, and placed there for a very good reason. I would like to take the opportunity to highlight some of our concerns and reactions to the TWIC proposal, especially as it has now been modified.

There is little doubt TSA had a challenging task in drafting the TWIC NPRM. While we appreciate the fact that in many regards the NPRM follows the mandates of Section 70105, unfortunately there are areas where we believe the rule may have fallen short. Fulfilling Section 70105 and striking a balance between security and fairness is a key part of the process, and not mutually exclusive. To the contrary, a workable, reasonable, and fair TWIC process will only enhance transportation security, and should be a proposed rule that can be altered to better achieve this objective.

I. The ILWU is concerned with the following areas;
- Disqualifying Offenses
- The Waiver Process – including the use of Administrative Law Judge (ALJ) and "subjective" decisions
- Document Cost
- Definition of Transportation Security Incident
- Privacy Rights

II. The ILWU is very concerned with ;
- Trucker Identification & Background Checks
- Vessel Crew Identification & Requirements

III. The TWIC Itself – Will the TWIC Work as now Proposed?
- Non-tested Hardware & System Modifications
- Climate and Inclimate weather,
- Cargo and Commercial Delay Relating to Unduly Infringing on the Flow of Commerce

Disqualifying Offenses

The ILWU, along with many others in the stakeholder group (from all sides of the "fence,") remain concerned that that the list of felony offenses that will disqualify a worker from holding a maritime TWIC is too broad, too vague, and not adequately focused on eliminating true security risks. Section 70105 is pretty clear. It states that an individual may not be denied a security card unless the individual has been convicted within the past seven years or released from incarceration in the last five years of a felony "that the Secretary believes could cause the individual to be a terrorism security risk to the United States." We maintain that some of the disqualifying offenses listed in Section 49 CFR 1572.103 are too broad and go beyond the mandate and it's limitation's. Specifically, there are interim felonies that do not tie a person to terrorism or to terrorist tendencies (as does treason for example,) and that should not be on the list. Additionally, except within very explicit circumstances, once a person has paid for his or her crime, unless there are extenuating circumstances accompanying the particular felony relating to terrorism, there is no good reason to deny the individual his or her right to a job on the waterfront.

Section 70105, in looking at criminal records, insures the Secretary may only deny a card to someone posing, or who could pose, a terrorism security risk. But consider for a moment, by way of example, where the NPRM is saying that felonies involving "dishonesty, fraud or misrepresentation" make an individual at least an initial terrorism security risk. If a worker is convicted of a felony in writing bad checks, wouldn't that

qualify as a crime of "dishonestly or fraud" under the broad exclusionary terrorist language?" While a financial institution may not want to hire that person, that does not make the individual a terrorism security risk, that would now make that person unable to work in a port. **There needs to be a clearer nexus between terrorism security and the crimes that will disqualify an individual from holding a maritime TWIC.**

In the NPRM, TSA and Coast Guard note that they are adopting the disqualifying offenses currently in place for the federal Hazmat program. While we agree that the two programs may, for reasons the regulatory agencies have yet to make clear, be similar, it must be remembered that the Hazmat program and the maritime TWIC program are governed by two different statutes. Specifically, Section 1012 of USA Patriot Act (codified at ____ USC 5308(a)) grants TSA broader discretion in deciding what crimes will disqualify someone from the industry and how far back the criminal record should be examined. Section 70105(c) places limits on the Secretary for the maritime program – *only those crimes that make someone a terrorism security risk to the United States should be included.* The ILWU believes it's critical that the list of criminal offenses be consistent with the MTSA standard. While TSA claimed it was adopting such an approach, we continue to believe that the crimes adopted for the Hazmat program and proposed for the maritime TWIC, do not in fact meet the standard established by Section 70105.

In response to calls requesting limiting the list of the disqualifying crimes, TSA has repeatedly stated that such refinements are unnecessary because a worker can always apply for waiver. While we appreciate the inclusion of the waiver process in Section 70105, it should not be used as *excuse* to adopt an overly broad list of felonies.

Deeming someone a "terrorism security risk" is not a decision that can be casually rendered; the burden alone to overcome the "terrorist" label (once rendered) will be enormous. While TSA may be able to report that it is granting waivers in the Hazmat program, this is not the TWIC program and there are big-time differences between the two. The Haz-Mat truck driver simply can decide not to apply...and can still continue working by transporting non-"haz-mat" cargo. Who knows how many truckers have simply not chosen to apply for the endorsement in the first place because of disqualifying offenses, immigration status, or information that could lead to personal problems? With TWIC, there is no such decision. Either you apply or you forfeit your job.

Furthermore, TSA will need to review and process the criminal histories of TWIC applicants on an *extremely tight deadline*, one of the first signs of general systems overload. As many of the comments have shown (at all three of the only public comment venues offered up,) it is obvious that the TWIC program is now being "fast tracked." On top of the other procedural challenges inherent in the process, it makes little sense to overload the waiver process with individuals that should never have been disqualified in the first place.

Waiver Process and ALJs

Having worked directly with members of Congress and their staff in discussions and negotiations that eventually led to the inclusion of the 70105 language and a waiver

process was a major priority of the ILWU. We are concerned however; about a process that requires workers to apply back to the same agency that determined that that individual was a security risk in the first place. Given the public's anxiety regarding terrorism and the insular nature of this process, we are concerned that TSA might reject waivers that otherwise may have been meritorious.

In attempt to address this problem, we've requested to allow workers to have their waiver cases heard, at some point, before an Administrative Law Judge (ALJ) at a hearing on the record. This would allow port workers to make their case in front of an impartial decision-maker not bound either by political pressures or agency interference. In addition, an added benefit would be that ALJ decisions would help to establish a system of "base-line" precedent, helping to better define what constitutes a terrorism security risk. This would introduce a level of fairness and consistency to the TWIC program by harmonizing American worker's rights and national security. There is currently a move in Congress for redress on this point included in the pending Coast Guard Reauthorization Conference Report (H.R. 889.) While we understand that the Conference Report is being held up for unrelated reasons, the **bipartisan support** for the introduction of ALJs into the process is clear. The ILWU would specifically like to thank Senator Stevens (R) from Alaska, and Senator Inouye (D) from Hawaii for their help on this issue.

Why would we not include an ALJ in the TWIC program? Remarks made by TSA and the Coast Guard have stated they will alter the proposal if Congress changes the law. But realistically speaking, when we start talking about taking away an American's right to feed and support his family, we are treading on dangerous "ethical" grounds. Every single American has the right to work any job he desires, unless of course, he or she has somehow compromised this right. Who less than an ALJ should be allowed to make this decision? Would you like a regulatory agency, with the notorious level of politics known to permeate the system, to decide your fate? While we have every confidence that Congress will act, why refuse to include ALJ's in the first place? **This is just too serious an issue.** Because TSA and the Coast Guard clearly have the discretion to include ALJs in the process, we sincerely hope they will realize the seriousness of the need and incorporate it into the system. Whatever happens, cases must be heard and decided as expediously as possible so that workers are not unjustly barred from returning to work.

Application of Waivers to Subjective Decisions

We are also concerned that the NPRM's waiver process does not apply to security threat assessments made by TSA for subjective reasons under Section 1572.107. Under this Section, TSA can disqualify someone for criminal offenses that are not on the disqualifying list, if the TSA determines that other convictions are "extensive," if the conviction is for a "serious" crime, or if the person was imprisoned for over a year. Putting aside for a minute our concerns with the broad and subjective criteria, we do not understand how TSA is implementing this without allowing workers to seek waivers as they do for crimes listed in Section 1572.103.

More to the point, Section 70105(c)(2) of the MTSA specifically mandates that TSA afford a waiver process for all reasons a worker may be disqualified from holding a transportation security card. We understand that TSA does not afford waivers under the

Hazmat program for disqualifications for subjective decisions. And while one may object to that decision in the Hazmat based on policy grounds, the case here is different – for the maritime TWIC, the waiver is a statutory right and cannot legally be denied by TSA at its discretion. We would expect TSA to make this change as it finalizes the rule.

Cost of the TWIC

That the TWIC program passes the costs on to the worker poses several questions. The security assessments and background checks mandated in this proposal are considered necessary to enhance the security of our nation's ports as part of the overall national effort to fight terrorism. Given the reality of the priority and national security in general, why isn't the government, and not the American worker absorbing the costs of the program. We understand that the DHS Appropriations Act (P.L. 108-90, Section 520) directs TSA to "charge reasonable fees for providing credentialing and background investigations in the field of transportation." On this basis, we would respectfully ask Congress to lift this appropriations rider and allow the federal government to fund the program in a reasonable manner. However, even with the rider in place, there is nothing requiring workers to absorb the cost of the TWIC – it simply states that "reasonable fees" be charged. As it now stands, the TWIC card and the accompanying background check have essentially become a condition of employment. According to the program, seaports and related facilities will be more secure through the access control procedural placement of the "direct" and "biometric" card readers. If the federal government refuses to step in and fund this security mandate then logically, it should fall to the employers to fund. Employees will still have to go through the time and effort to apply for the TWIC and may incur additional expenses when or if an appeal and waiver are needed. It really isn't reasonable or fair to ask a worker to pay for a security mandate. In the past, for example, would the government even consider requiring military personnel to pay for their military ID?

There is also the question about how the TWIC cost has grown beyond all expectations. Originally envisioned to be about $80.00, the current cost of $140.00 per card is very expensive. Many within the industry have commented that this is sounding more and more like an govt. agency financial boondoggle. Is this a case where the public is, once again, paying for the proverbial $500.00 hammer or a $200.00 ashtray? Or is this a case of the lobbyists and corporations making profit off the backs of hard working Americans who are forced to buy it or not work? If this is the case, it's wrong and should be exposed as such. No American worker should be exploited simply because they can.

Transportation Security Incident

Under Section 70105(c)(1)(A)(ii) of the MTSA, an individual will be denied a maritime TWIC if he has committed a felony, within the last seven years, that causes "a severe transportation security incident." The MTSA defines this term to include a security

incident that results in a "transportation service disruption" or an "economic disruption in a particular area." Both the Hazmat rule and the maritime TWIC NPRM have made a "transportation security incident" a permanent disqualifying offense with no waiver opportunity. As previously stated the ILWU is concerned with the broad definition of the offense. In this case, it could be interpreted to include such a wide range of activities that, while they may be disruptive to commerce or transportation, they might not necessarily be so serious as to permanently disqualify a person from holding a TWIC. We are pleased that Congress, again in the SAFETEA-LU legislation, included a provision that attempts to limit the reach of this provision and TSA has modified its rules accordingly. Nonetheless, we remain concerned that the term could be misused and we urge further clarification as the process moves forward.

Privacy of Information

Maintaining the privacy and confidentiality of the information collected and generated by the TWIC process is crucial. Towards this end, Section 70105(e) includes a specific mandate that "information obtained by the Attorney General or the Secretary under this section may not be made available to the public, including the individual's employer." Consistent with this requirement, any and all information gathered from the use of the TWIC must not be shared with the employer in any manner. The TWIC program was conceived and mandated by Congress to enhance the security of the nation's ports. For this to succeed, it must remain focused solely on that objective, and not be used for any other reason. This issue is a critical one, and as such should be addressed in the final rule.

SECTION B. Fairness of Application

Truckers

Truckers are the largest occupational group of workers within the marine terminal facilities; they deliver and pick-up cargo and containers and utilize terminal access control far more than any other group. OF all the work groups in the ports they may also be the most difficult to "credential." There are up to ten times the number of truckers operating in Southern California's ports than any other work or occupational group. This is easily evidenced by the thousands of gate moves executed by each of the fourteen Southern California marine container terminals operating there. **Because the majority of truckers are "owner-operators," an inherent difficulty exists in creating a truck driver master data list.** This was just recently evidenced by the inability of the federal regulatory agencies to successfully "vette" this one occupational group. This must be done.

In the recent anti-terrorist "vetting" process, the trucker group was not included, simply because it was too difficult, a significant fact considering this is the largest occupational group in the port and has already been identified as a risk in past risk and threat assessments. Why this happened is completely mystifying. Since when has US federal agencies failed to do something because it was too difficult? The foundation of

the TWIC program is clear, "**all persons entering a marine terminal must hold a TWIC**." If TWIC is allowed to evolve into a "selective" ID program where some have to have the card and others don't, there will be no reason to have it at all. Without this overarching principle, this process will end up being known as the federal port ID program that failed, including the millions of public tax dollars that will be called to accountability.

Full and equal application of the TWIC to **all** desiring access to a US marine terminal is necessary and a must if this program is to succeed. And as far as the original mission statement is concerned, TWIC has never changed. Truckers must be checked just as any other group. And the background checks must be required of everyone. Statements like "well, it's going to be difficult to create a master list of truck drivers," or "many of the driver's are not citizens and how are we going to accomplish background checks in foreign countries," simply won't wash. They are but examples of some of the problems that simply must be solved. These are not new problems, but ones that the regulatory community, including D.O.T., TSA, and Homeland Security, have been aware of for a long time.

It should be made clear that each aspect of the credential process must apply fairly and evenly to everyone involved. Everyone must be subject to the same criteria, there should be no "claimed identity" status for anyone and, before the program is ready for full implementation, all persons desiring access should have already undergone exactly the same background checks and held subject to the same disqualifying offense criteria. The TWIC program should not be allowed to begin until the majority of all maritime workers as defined, have been run thorugh the TWIC process. Persons of foreign birth (or with resident status) must have exactly the same background check run on them that is required of American citizens.

Vessel Crews

At the present there is no master international ID card for the majority foreign vessel crewmembers entering US seaports. Will foreign crews be required to hold the same TWIC; they are entering and leaving the marine facilities as everyone else who must have card. Little known or discussed is how foreign vessel crewmembers regularly exit and access vessels while in port, and specifically, how they move throughout the terminal, sometimes with no formal ID. There are terminals in the ports where a second exit gate exists from which crew members enter and leave the facility along with other port workers, other than the main gate which they should be using. Crewmembers regularly exit vessels looking for pay phones, as they also regularly walk around the vessel checking vessel moorings and draft. There are many instances where crewmembers could easily disappear from the vessel, be picked up in a truck and transported out the main-gate onto city streets and no one would ever know.

Once again, this goes back to equal application under the law. As with the 70105 Section surrounding terrorism, the point is to make US marine terminals as secure as possible. Truckers and vessel crewmembers are, security-wise, the access control "weak link." There are a number of situations and potential security disruptions and dangerous scenarios that could truly be exploited by those wishing to do harm to our country.

As important as anything else is, "will the TWIC system work as now modified?" As there always are multitude of problems that accompany any new program implementation, this will also happen with TWIC. The question is however, "will this be magnified because the prototype testing was not done on the same systems and criteria now called for." What happens when these systems, ones that were not tested, malfunction or do not work as advertised? The "direct" card reader is a great example. From the start, this was never seriously considered as a system, yet we now see that TWIC cardholders are going to have to slide their cards through a "direct" reader. Further, what about the expensive biometic reader's that are now going to be used in conjunction *with* the direct reader? New systems never operate at 100% efficiency, or reliability. There are a number of problems that the use of the readers may create. First, the biometric readers could break down, and cause such significant problems that eventually they may have to be abandoned. If that happens what we'll be left with nothing more than an expensive "direct" reader scanning a magnetic strip; which is almost exactly what we have now. And the government will have wasted almost a billion dollars on a card that has no guaranteed personal identifier, and thus able to be used by anyone who has nothing more to do than slide it for access. How would you stop one individual from using another's card?

As importantly, what will the cost be in terms of infringing on cargo flow and commerce? Recent estimates dealing with the Coast Guard delays related to the "random" at sea inspections have put the cost of container ship delays at $40,000.00 per every hour lost. This recently became a huge issue when it was discovered that the Coast Guard in different regional areas were apparently operating contrary to one another. Some commands were notifying carriers and shippers about specific "impending" random inspection's, while others were horrified to find that the supposedly random and secret inspections were not so *random* after all. What's important is that **this occurred because of the intense pressure brought to bear from shippers concerned about the costs surrounding cargo delay.** What's going to happen when a systems glitch or breakdown causes an entire day to be lost because labor for a vessel was turned around at the gate because of a broken or improperly functioning system? What about the weather and climate concerns regarding the expensive and sensitive hardware proposed? Full-time salt air saturation and precipitation are known to damage these kinds of systems. Many of these concerns and considerations were not dealt with in prototyping because the systems now proposed are not the same as they were then.

It appears, after hearing all the comment from both industry and labor alike, that the TWIC is not ready for deployment. The test-bed phase that originally took so long did so because of the extensive extenuating factors TWIC is dependent on and that no one originally planned for. Now that we have government demand for rollout for their own reasons, is it possible that TWIC be being rushed to implementation, when certainly it's not because it's ready. The majority of public comment clearly has reflected this, with most coming from the industry supply chain stakeholders themselves. It's pretty clear that the public, industry, labor, port authorities etc., while all voicing strong support for national security, are not sanctioning the untimely and therefore improper decision regarding the TWIC implementation. These are the guys on the job, they're the men and women who move the cargo, and if anyone knows, they know. Considering this, why is the government so strongly motivated to move forward? Will the Administration

continue to ignore comment from those most intimately "industry" involved just to say that "we've done something?" And now, most important, is the report from Dept. of Homeland Security Inspector General on TWIC reflecting many of the issues we have raised.

The Port and Intermodal Systems Center for Enhanced Security (PISCES)

A "White Paper" Abstract Summary

The Port & Intermodal Systems Center for Enhanced Security (to be known as **PISCES**), a California State University (CSU) multi-campus collaborative partnership, includes the following CSU system founding members:

- California Maritime Academy (CMA), Vallejo, CA
- California State University, San Bernardino (CSUSB)
- California State University, Long Beach (CSULB)
- California State University, Los Angeles (CSULA)
- San Diego State University (SDSU)
- California Polytechnic State University, San Luis Obispo (Cal Poly SLO)

The members have formed **PISCES** in response to a Congressional legislative initiative in the *Coast Guard and Maritime Transportation Act of 2004* to provide a long term strategic and collaborative approach to address port, intermodal, and other transportation-related critical infrastructure, efficient goods movement & national security issues.

Each of the founding members brings unique established capabilities and resources to the common venture:

- **CMA** has unique knowledge of maritime domain and situational awareness and training applicable to the security of the nation's ports and harbors garnered over a 75 year history of providing academic & professional education to merchant mariners;
- **CSULB** through its Center for the Commercial Deployment of Transportation Technologies (CC-DoTT) and Center for International Trade and Transportation (CITT) has developed a national reputation for expertise in goods movement, and port and supply chain security in collaboration with **CSUSB** and the Collaborative Agent Design Research Center at **Cal Poly SLO**;
- **SDSU** created and operates, in partnership with **CSULB**, the Center for Commercialization of Advanced Technology, a DOD funded program, which employs a proven methodology of soliciting, screening, evaluating and advancing promising technologies that address both homeland defense and homeland security priority needs;
- And **CSULA**, through the College of Health and Human Services and its School of Criminal Justice and Criminalistics, has a nationally recognized criminalistics program with experts in various areas of forensic science;

PISCES members will commit their respective resources and capabilities - along with other potential future consortia members - to identify port and intermodal security capability gaps and to mitigate these vulnerabilities in the nation's strategic ports and supply chain through the development and application of needed education, training, and process programs, and the testing, validation and integration of advanced technologies in port and intermodal security systems across the nation; and

PISCES, by design, will engage on all of these issues with primary mission, goals and objectives that include several critical focus areas within the Port and Intermodal operational arena. These areas include:

1. As central evaluation and test center, identify, validate, demonstrate and implement emergent technological advancements originating from academia, industry, government, and individual entrepreneurs to meet the critical national problem of improving port and intermodal homeland security. As a development and Beta Test center, **PISCES** will focus on practical, rapidly deployed and cost effective solutions tailored to the rigors of the operational environment – solutions that work, are relatively simple to operate and that require the least in terms of capital investment and long term maintenance or replacement expense.

2. Capitalize upon and streamline the modification and translation of DOD developed technology, policies and procedures for use in the civilian commercial port and intermodal environment.
3. Address security issues and solution identification in the maritime and port environment within the full context of preserving, protecting and strengthening the national distribution system, as well as associated quality of life issues including infrastructure, environment, economics and transportation mechanics that in totality comprise the complete spectrum of concerns – and must therefore be fully considered when implementing any sustainable solution.
4. Working with public and private, local, state, regional and federal stakeholders, act as a nexus for the de-confliction and integration of practical, sustainable, and workable all hazard emergency plans.
5. Information and Intelligence Fusion, particularly in the area of collection, development and distribution of usable and timely information extending to the commercial and operational elements of the port.
6. Identify capability gaps – resource, technological, operational, educational, training, and planning -- and mitigate vulnerabilities in the nation's strategic ports and associated national distribution network.
7. While situated and targeted to address issues in the Pacific Area, the **PISCES** will create procedural and operational templates that will be applicable throughout the nation, and internationally – particularly in so far as uniform and sustainable implementation of the IMO International Ship and Port Security Code (ISPS Code) and the U.S. Maritime Transportation Security Act of 2002 (MTSA 2002) – helping to ensure the establishment of a global security umbrella for the United States and its critical trade partnerships.
8. Once identified and tested, provide a coordinated, practical, efficient and cost effective training and continuous improvement system that delivers uniform, comprehensive initial training, currency validation and fundamental assumption and capabilities testing across transportation modes for security professionals, first responders (LE, FF, and EMS), emergency planners, and transportation specialists

As described, **PISCES** will clearly support and enhance the goals and objectives set forth under ***DHS's OPERATION SAFE COMMERCE*** program. Now about to move forward into its fourth phase, this program is attempting to address communications and information sharing, domestic and international shipment tracking and development and deployment of technologies and systems that work to assure maximum security from point of origin to final destination and every waypoint in between. Capabilities gaps targeted at improving inoperability, communications and integration of practical security processes, procedures and planning that also balance and lessen potential negative impacts to goods movement represent a fundamental cornerstone of the PICES mission and *highlight a possible key focus segment for the fourth phase* of ***OPERATION SAFE COMMERCE***. Critical to the ultimate success of any security program – and currently under supported – are also the practical necessity of testing any proposed procedure or plan evolving from these processes by integrated training and direct exercise experience as a integral part of the continuous improvement and readiness process.

Also fundamental to overall success of security and operational integrity will be the smooth integration of security and goods management programs across intermodal boundaries. Therefore PICES will target and configure its research, process and program development, training and execution guidance to support not only DHS programs but also ***Department of Transportation (DOT)*** programs such as the newly announced ***Framework for National Freight Policy*** and particularly *Objective 6* to this framework that speaks to ensuring a balanced approach to security and efficiency in all freight initiatives across regulatory and departmental boundaries.

Seaport Security

Enhancing maritime security and protecting America's seaports from acts of terrorism and other federal crimes is a top priority for AAPA and U.S. port authorities. Protecting America's ports is critical to our nation's economic growth and vitality, and an integral part of homeland defense. Ports handle 99% of our overseas cargo volume, enable the deployment of our military, and serve as departure points for millions of cruise passengers annually.

Port security is a shared responsibility with the federal government, with the Department of Homeland Security, taking the lead. Key agencies in this effort are the U.S. Coast Guard and Customs and Border Protection.

Partnership Approach

Protecting our international seaport borders is a responsibility shared by the federal, state, and local governments, port authorities and private industry. AAPA and its member public ports, along with their terminal operators, work closely with the Department of Homeland Security (DHS) and other federal agencies to enhance maritime security and to participate as strong partners in protecting our homeland.

Ports are located on international borders, and the federal government is responsible for inspecting and approving international cargo and passengers, and has oversight for facility and vessel security. For port facilities, U.S. Coast Guard reviews and approves all maritime facility security plans.

Customs and Border Protection (CBP) pursues a layered security strategy in which 100% of the cargo is screened before being loaded on a vessel, and in larger container ports CBP works with foreign countries to inspect all suspect cargo overseas. CBP also has other non-invasive security systems available in many U.S. seaport facilities. Cargo cannot enter the U.S. unless it is approved for entry by the CBP. Once the cargo is cleared for entry, port authorities and terminal operators are responsible for moving the cargo off the ship, storing it on the facility and loading it on trucks or rail to move to another destination.

Port Security Grants Are Vital

To help make improvements quickly, Congress also established the Port Security Grant program. Ports apply directly through this competitive grant program to DHS for assistance to make facility enhancements. For this program to make the greatest impact on enhancing port security, the federal government must:

- Provide adequate funding;
- Open the program up to all MTSA-covered facilities;
- Maintain a separate, dedicated program;
- Release funds more quickly from the program

$400 Million Needed in FY'06 Funds

When DHS developed regulations for the port industry in 2002, the U.S. Coast Guard estimated that port facilities would need to spend an estimated $5.4 billion over 10 years for the base requirements alone. Without significant federal support in FY'07, improvements will take more time and new advancements may not be implemented. Significant homeland security funds are needed to speed the protection of this vital transportation asset. AAPA recommends a funding level of $400 million a year. Compared to

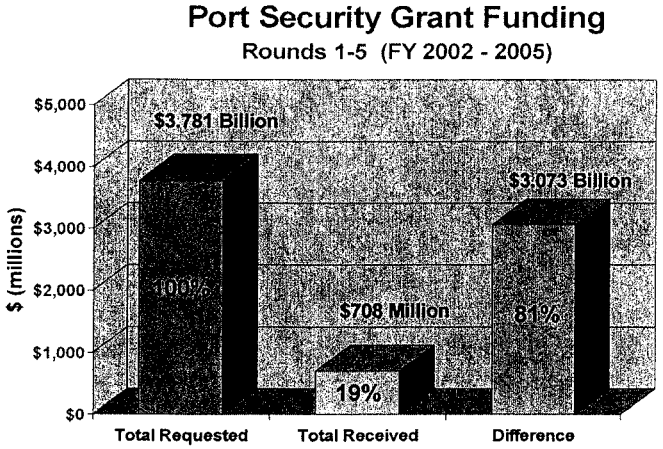
the billions of federal dollars allocated to airports, first responders, and science and technology, this is a modest investment in the nation's infrastructure.

While Congress has provided funds in several appropriations bills since September 11 (see chart), the funding is far short of the identified need. In the first five rounds, port facilities have received only 20% of what was requested. Limited funds mean slower progress.

A Dedicated, Separate Fund Should Be Maintained

In the FY'07 budget, the Administration also proposed eliminating this program and lumping ports into a proposed Targeted Infrastructure Protection program, along with bus, rail and other infrastructure. AAPA is strongly opposed to this merger – this is not the time to dilute our focus on port security.

A dedicated port security grant program must be maintained whereby ports can apply directly to DHS for these funds. Ports are the only entity within this proposed program that must meet regulatory mandates. It would also merge an international border program (ports), with programs to protect domestic assets. A dedicated fund would assure resources are allocated for this critical asset in order to avoid the disruption of cargo movements through ports.



Grant Eligibility

Due to the limited funds and the focus on risk, DHS made a policy decision to limit eligibility. Limiting eligibility might give the impression of a class of perceived underprotected ports. AAPA supports a risk-based system and believes all facilities covered by the MTSA should be eligible to apply.

Resources for Federal Agencies

Port security missions have placed many new requirements on federal agencies, especially the U.S. Coast Guard and CBP. While both have addressed these new challenges well, Congress needs to carefully evaluate whether the resources are adequate to do the job. Cargo and passenger volumes through ports will increase significantly in the coming years and DHS must be ready.

DHS also needs the funding to quickly implement the Transportation Worker Identification Credential (TWIC), which was mandated in 2002 under the MTSA. To qualify, the law requires that all individuals who have unescorted access to a secure area of a port facility or vessel undergo a background check to ensure they do not pose a terrorist security risk. DHS must move more quickly to implement this system nationwide.

No New Taxes

The maritime community already pays billions of dollars in user fees and taxes to the federal government, including $17.5 billion in Customs duties. Maritime cargo provides approximately 70% of the yearly Customs collections. AAPA believes that Customs duties should be used as a source of security funds if Congress seeks a dedicated source of funding. March 2006

To learn more, visit AAPA's web site at

www.aapa-ports.org

TESTIMONY OF

MATTHEW BETTENHAUSEN, DIRECTOR
CALIFORNIA OFFICE OF HOMELAND SECURITY

BEFORE THE

JOINT COMMITTEE ON EMERGENCY SERVICES AND HOMELAND SECURITY

AND THE

SENATE COMMITTEE ON TRANSPORTATION AND HOUSING SUBCOMMITTEE ON CALIFORNIA PORTS AND GOODS MOVEMENT

AUGUST 11, 2006

Madam Chair and Members of the Joint Committee on Emergency Services and Homeland Security and the Senate Subcommittee on California Ports and Goods Movement: Thank you for the opportunity to testify before you. My name is Matthew Bettenhausen and I am the Director of the California Office of Homeland Security (OHS).

Port security is a high priority for this Administration and Governor Schwarzenegger is committed to ensuring California is a leader in port security developments. About 90 percent of all world cargo moves by container and almost half of incoming trade, by value, arrives in the U.S. by sea containers. There are approximately 9 million cargo containers that arrive and are offloaded at U.S. seaports each year. Maritime infrastructure and its systems are increasingly becoming targets of illicit activities. Ports are often a major focus for criminal activity including drug trafficking, cargo theft, the smuggling of contraband, including foreigners coming illegally to the U.S., and acts of terrorism.

The federal government has made significant strides in providing leadership and guidance for the protection of maritime infrastructure and its systems. In September 2005, the Department of Defense (DOD) and the Department of Homeland Security (DHS) released a comprehensive National Strategy for Maritime Security which integrated different federal department-level strategies and sought to ensure their effective implementation. To support the National Strategy for Maritime Security, DOD and DHS developed eight national implementation plans to address specific threats and challenges. One of these plans, the Maritime Infrastructure Recovery Plan (MIRP), was established in April 2006. The MIRP establishes procedures and standards for the recovery of maritime infrastructure following a national Transportation Security Incident (TSI). A TSI is defined as any incident that results in a significant loss of life, environmental damage, transportation system disruption, or economic disruptions to a particular area. A national TSI is a TSI that has been declared to be an Incident of National Significance (INS), an actual or

potential high-impact event that requires a coordinated and effective response by a combination of federal, state, and local governments and/or private-sector entities in order to save lives, minimize damage, and provide for long-term community recovery and mitigation activities. The Secretary of Homeland Security has the authority to declare an INS. The MIRP reflects the National Response Plan's (NRP) organizational concepts and the use of the Incident Command System (ICS) and unified command procedures. The MIRP provides guidelines for those involved in the decision making process to maintain the operational capabilities of the nation's Maritime Transportation System (MTS) and restore transportation capabilities if compromised.

The NRP and the National Incident Management System (NIMS) are two documents intended to provide a single, comprehensive approach to incident management. These documents were produced in response to Homeland Security Presidential Directive 5, which stated that the Secretary of Homeland Security is responsible for coordination of the federal preparations, response and recovery from terrorist attacks, major disasters and other designated emergencies. The NRP outlines how the nation would plan and respond to an INS. It forms the basis for how federal departments and agencies would work together and coordinate with state, local, tribal governments and the private sector during incidents. NIMS is intended to provide a standard system for federal, state, local and tribal governments to work together to prepare for and respond to incidents. NIMS utilizes ICS as a standard incident management organization for the management of major incidents. As a condition of receiving federal preparedness funding assistance in Fiscal Year (FY) 2007, state, territorial, tribal and local entities must complete NIMS related training during FY 2006.

In the event of a port security incident in California, the Incident Command System (ICS) provides the framework for organizing response and recovery activities. The ICS is a standardized, on-scene management concept. It is a flexible system that can meet the needs of incidents of any kind or size and allows personnel from different agencies to meld into a common management structure. The ICS outlines procedures for controlling personnel, facilities, equipment and communications. It is designed to be used through the life cycle of an incident. The ICS organization is developed upon five major functions – Incident Command, Operations, Planning, Logistics and Finance/Administration. Incident Command sets the incident objectives and strategies and has overall responsibility for the incident. OHS staff are not first responders and therefore would not play an operational role in response to an incident; staff would integrate into the Planning Section. This section is responsible for preparing and documenting the Incident Action Plan, collecting and evaluating information, and maintaining resource status and documentation for incident records. OHS staff would be heavily involved in coordinating and facilitating intelligence information sharing between the Sections.

Protecting California's seaports from acts of terrorism and other crimes are of vital importance to both the State and the national economy. California's seaports handle about 43 percent of the nation's goods that arrive by sea and are home to a major Naval Station in San Diego and a large cruise ship industry. The majority of maritime traffic comes through the neighboring ports of Los Angeles and Long Beach, which handle 32% of the nation's container throughput. The National Strategy for Maritime Security calls for a layered security approach, a strategy which California is following to protect its coast and ports. The many layers to California's risk

management strategy include a combination of federal efforts and grant funding and State initiatives and funding, which are as follows:

1. The Customs-Trade Partnership Against Terrorism (C-TPAT) is a joint government-business initiative to build cooperative relationships to strengthen supply chain and border security. There are over 2,500 C-TPAT partners that have agreed to protect the supply chain.

2. The U.S. DHS screens information on nearly 100% of all containerized cargo before it arrives in a U.S. port. Through the Container Security Initiative (CSI), U.S. Customs and Border Protection (CBP) inspectors are placed at the world's top seaports where they work with their foreign counterparts to screen and label "higher-risk" or "low-risk" cargo before it is shipped to other ports. The CSI program also calls for using "tamper-evident" containers. To be eligible to participate in the CSI program, nations must, at a minimum, utilize non-intrusive inspectional (NII) equipment, including gamma or X-ray imaging capabilities, and radiation detection equipment to inspect cargo originating, transiting, exiting, or being transshipped through a country. The program has been implemented in as many of the top 20 foreign containers ports as possible, which account for nearly 70%, over two-thirds, of all cargo containers arriving at U.S. seaports.

3. The 24 Hour Rule requires electronic transmission of advance cargo manifests from U.S. bound sea carriers one day in advance of loading. Early industry reports show that this rule is aiding productivity as well as security. The information provided by the 24 Hour Rule is then run through the Automated Targeting System. This information is compared against law enforcement data, latest threat intelligence, and the ships' history.

4. Advanced technologies are being used to screen and examine cargo and enhance worker identification security efforts. Radiation Portal Monitors (RPMs) scan 100% of the trucks and containers leaving California's ports. Higher-risk shipments are physically inspected for terrorist weapons and contraband before they are released from the port of entry. The Transportation Worker Identification Credential (TWIC) program will add an additional layer of security by establishing a standardized process for issuing identification credentials to transportation workers. Transportation workers would use TWIC to access secure areas of transportation facilities. TWIC verifies the holder's identify by linking the individual's claimed identify and background information to the holder's biometric information stored on the card. A pilot program for TWIC has been successfully completed and the Transportation Security Administration (TSA) is in the process of promulgating regulations.

5. California's ports have received $132.4 million in federal port security grants from DHS. In administering these funds, OHS partners with the U.S. Coast Guard and law enforcement. Funds are used to enhance security by providing ports with patrol boats, surveillance equipment, and command and control facilities. For FY 2006, over $168 million is available through the Port Security Grant Program. Eight California ports -- Los Angeles, Long Beach, Oakland, Hueneme, Richmond, San Diego, San Francisco and

Stockton -- are eligible to apply for funding. California's allocation will be determined at the end of a competitive process.

6. Last year, the Governor directed $5 million to help secure 11 California ports: Hueneme, Humboldt Bay, Long Beach, Los Angeles, Oakland, Redwood City, Richmond, San Diego, San Francisco, Sacramento and Stockton. These funds are directed towards increasing domain awareness and enhancing information sharing. These operations centers will be connected with the State Terrorism Threat Assessment Center (STTAC) and the four Regional Terrorism Threat Assessment Centers (RTTACs). This will ensure the State has the capability to share information, detect terrorist plots, and disrupt criminal acts. The $5 million comes from the State's share.

7. The San Diego Sector Command Center-Joint (SCC-J) is a joint operations center partnership between the Navy, the Port of San Diego, and the San Diego Harbor Police. The SCC-J is active 24/7 and will merge local and federal monitoring and surveillance systems for vessels, swimmers and divers. This and a similar center in Norfolk, VA are the first in the nation to have this type of federal and local cooperation to maximize port security communication and collaboration.

8. In the November 2006 General Election, California voters will have the opportunity to vote on Proposition 1B or SB 1266 (Nuñez/Perata), the Highway Safety, Traffic Reduction, Air Quality, and Port Security Bond Act of 2006. This proposition authorizes $19.925 billion in bonds for specified purposes. In regards to port security efforts, $3.1 billion would be authorized for a California Ports Infrastructure, Security and Air Quality Improvement Account. The Act would also authorize $100 million in grants to be distributed by the Office of Emergency Services for port, harbor, and ferry terminal security improvements. While OHS' role is not mentioned specifically in this proposition, the passing of this proposition would have a direct impact on port security efforts. OHS remains an active stakeholder in this process.

9. From August 15-17, 2006, OHS will be hosting a Transportation Infrastructure and Maritime Forum with the U.S. Eleventh Coast Guard District regarding "Moving the Safety and Security of California Forward". During the three-day conference, attendees will have the opportunity to attend a number of workshops and panel discussions. Topics will include building security partnerships with the Transportation sub-sectors, port recovery planning, science and technology for cargo and port security and TWIC implementation. One of the main goals of the workshop is to inform the development of statewide maritime security strategies to complement the National Strategy for Maritime Security.

10. Finally, a number of maritime security exercises have been held at the ports of San Diego, San Francisco and Los Angeles/Long Beach.

    a. The Port of San Diego was the site of a three-part exercise named Exercise Bay Shield. This exercise was conducted by the San Diego Area Maritime Security

Committee (AMSC). California's three AMSCs – Northern California, Central California (including Los Angeles and Long Beach) and San Diego – were established to carry out the requirements of the Maritime Transportation Security Act of 2002 (MTSA). The MTSA directs the U.S. Coast Guard (UCSG) to conduct a vulnerability assessment of port facilities and vessels that may be involved in a TSI. Each AMSC is responsible for conducting a port area assessment and establishing a security plan. The committees are chaired by the USCG; OHS sits on all three committees. Exercise Bay Shield was intended to test the San Diego Area Maritime Security Plan. It began on July 19-20, 2005 with a two-day tabletop exercise that allowed more than 100 AMSC members to discuss coordination efforts in response to a possible TSI within the Port of San Diego. The second part of the Exercise took place on September 20, 2005 with a command post and surface deployment exercise to test the interoperability between local emergency operations centers. The Exercise concluded on July 26, 2006 with an eight-hour multi-agency drill simulating a major maritime incident involving a cruise ship. More than 30 agencies from around southern California, participated in the Exercise, including the USCG Sector San Diego, CBP, Immigration and Customs Enforcement, the Federal Bureau of Investigation, San Diego Harbor Police, and the County of San Diego.

b. San Francisco Bay's annual Area Maritime Security Exercise and Training Program (AMSTEP) exercise was held on August 2, 2006. The approximately eight-hour exercise, AMSTEP-Elevate Shield 2006, was held at various Bay Area venues including the emergency operations centers (EOC) for the City of Richmond, Contra Costa County, Chevron Oil Company, and the Port of Oakland as well as the Port of San Francisco's Department Operations Center (DOC), and the USCG Sector San Francisco's Sector Command Center (SCC). The Exercise focused on improving interoperability, and tested the Northern California Area Maritime Security Plan, associated USCG approved industry security plans, and the use of the USCG's HOMEPORT security information website. HOMEPORT is a secure Internet portal that will provide critical information and service delivery to the public, maritime industry, and USCG.

c. The Port of San Francisco was also the site of the first Port Security Training Exercises Program (PortSTEP) training exercise. PortSTEP was developed by the TSA and the USCG to help meet the mandates of the MTSA. PortSTEP is designed to provide maritime transportation security communities with training exercises, evaluations, and accompanying information technology products. The California Maritime Academy (Cal Maritime), a campus of the California State University, hosted PortSTEP's first exercise on August 18, 2005. The multi-agency command and control advanced tabletop exercise involved the TSA, USCG, Ports of San Francisco and Oakland, regional and local emergency planners, and first responders. A major objective of the exercise was to test the interoperability, coordination and emergency procedures of the San Francisco Bay

Area's Area Maritime Security Plan. A PortSTEP advanced tabletop exercise will be held for the ports of Los Angeles/Long Beach on September 26, 2006.

California has demonstrated leadership and initiative in developing other preventative security measures to add additional layers of security for our maritime infrastructure and systems. OHS has made important strides towards protecting our State's critical infrastructure and furthering collaborative efforts towards prevention, planning and response activities with our homeland security partners. We appreciate the dedication your committee members have shown towards furthering and supporting these efforts.

Thank you for your attention this afternoon.

OFFICE OF HOMELAND SECURITY

PORT SECURITY FUNDING IN CALIFORNIA

Total Port Security Funding to Date:

Program	Award
FY03 – FY05 Port Security Grant Program	$118 million
FY03 UASI Port Security Grant Program	$9 million
FY05 Homeland Security Grant Program	$5.4 million
TOTAL	***$132.4 million***

Federal Port Security Funding to Date:

Port Security Grant Program

A federal grant, awarded on a competitive basis, has been in place since 2003. The Office of Domestic Preparedness, Transportation Security Administration, Customs and Border Protection, the United State Coast Guard, and the Department of Transportation's Maritime Administration evaluate grant applications submitted by ports and facilities. The awards to date are as follows:

Round	National Total	California's Total
Round 1	$92 million	$17 million
Round 2	$168 million	$28.5 million
Round 3	$179 million	$33.6 million
Round 4	$49 million	$5.9 million
Round 5	$142 million	$33 million
Total	**$630 million**	**$118 million**

FY 2003 Urban Area Security Initiative Port Security Grant Program

The Emergency Wartime Supplemental Appropriations Act, 2003 provided $75 million in additional funds to urban areas to enhance port security. The federal Department of Homeland Security chose 14 urban areas across the nation. The Los Angeles/Long Beach ports and facilities were awarded $9 million.

California Port Security Funding to Date:

FY 2005 State Homeland Security Grant Program

OHS awarded $5 million to 11 California ports to enhance security. Additionally, the California Maritime Academy was awarded $400,000 to help fulfill the training and exercise needs identified by the three Area Maritime Security Committees. This funding came out of the State's share of this federal homeland security grant program.

Background on the FY 2005 California State Port Security Grant Program:

Governor Schwarzenegger dedicated $5 million out of the State's share of the Homeland Security Grant Program to enhance port security. OHS awarded this additional money to eleven ports:

Eligible Port	**Allocation**
Hueneme	$450,000
Humboldt Bay Harbor District	$150,000
Long Beach	$750,000
Los Angeles	$750,000
Oakland	$750,000
Redwood City	$150,000
Richmond	$450,000
San Diego	$750,000
San Francisco	$450,000
Sacramento	$150,000
Stockton	$150,000
Total State Port Security Grant	**$4,950,000**

These grants will be used to prevent terrorists from using improvised explosive devices, train port security personnel, and purchase communications equipment and physical security improvements such as cameras, lighting, fencing, underwater surveillance, and personal protective equipment for port first responders.

Summary of Specific Projects:

Port of Hueneme:

- Security fencing at the channel
- Barrier cable
- Security watercraft
- Vessel Traffic Identification System
- Emergency Siren
- Portable light towers
- Stationary search light

Port of Humboldt-Humboldt Bay Harbor District:

- Port Security Camera System
- Upgrading and replacement of perimeter fencing and install concrete barrier
- Purchase of fire/dewatering pump
- Portable lighting systems
- Purchase of night vision goggles-improve of surveillance capabilities
- Upgrade of secure VHF radio capability
- Purchase remote operated vehicle for underwater surveillance

Port of Long Beach:

- Purchase Handheld Explosive Detection Devices
- AVL-GPS Vehicle System-Monitor of patrol vehicles using computer software
- Vehicle Dash Mounted Mobile Video Surveillance System
- EOC Trailer and supplemental radio equipment

Port of Los Angeles:

- Mobile Explosive K9 Kennel
- K9 Equipment
- Surface Supplied Air Dive Helmets
- Under Water breathers
- Diver/Surface Communication System
- Mobile Decontamination Shelters
- Hazardous Material Response Software
- Under Vehicle Surveillance System
- Portable Explosive Detectors

Port of Oakland:

- Portable lighting
- Portable Programmable Signs
- Barrier Deployment Equipment
- Marine Patrol Boat
- Secure RFID Driver/Truck Tracking System
- Training for Facility Security Officers

Port of Redwood City:

- Install perimeter fencing and gates

Port of Richmond:

- Perimeter Security Fencing
- Lighting Systems Enhancements
- Surveillance System-CCTV Cameras

Port of San Diego:

- Interoperable Communications Equipment

- Fast response port security vessel and equipment
- Retain qualified professional consultant for development of port security master plan and additional security planning efforts.

Port of San Francisco:

- Port Security Cameras
- Portable lighting and sign system
- Upgrade of interoperable communication system
- Upgrade of laptop computers for EOC and Alternate EOC
- Additional port security fencing

Port of Sacramento:

- Emergency Lighting System
- Purchase emergency generators/portable light plant to power security cameras if facility power is disrupted.

Port of Stockton:

- Security fencing with automated gates

Joint Hearing
Joint Legislative Committee on Emergency Services and Homeland Security
and
Senate Committee on Transportation and Housing
"Securing California's Marine Transportation System:
Seamless Operational Security"

Friday, August 11, 2006

Long Beach, CA

Dr. Lawrence G. Mallon, Esq, Chair

Port Security and Consequence Management

AB 2043 CALMITSAC

Goods Movement and Port Security Study

California's First Comprehensive Port Security Survey and Capability Gap Analysis

Dr. Lawrence G. Mallon, Esq CSULB

And Captain Bruce Clark, USCG retd

CMA

w/assistance from SDSU Foundation

AB 2043 Port Security Survey Respondent Population

- Corporate/Company Officer/Director 11%
- Terminal/Facility Manager 30%
- Security Manager (CSO/FSO/VSO) 41%
- Emergency Preparedness Manager 15%

Target Respondent Population

- Port authorities (Cities, Counties, Special Districts)
- Small Craft Harbor Districts
- MTSA/PWSA Regulated Marine Terminal Facilities
- SOLAS/ISPS Regulated Vessel Operators

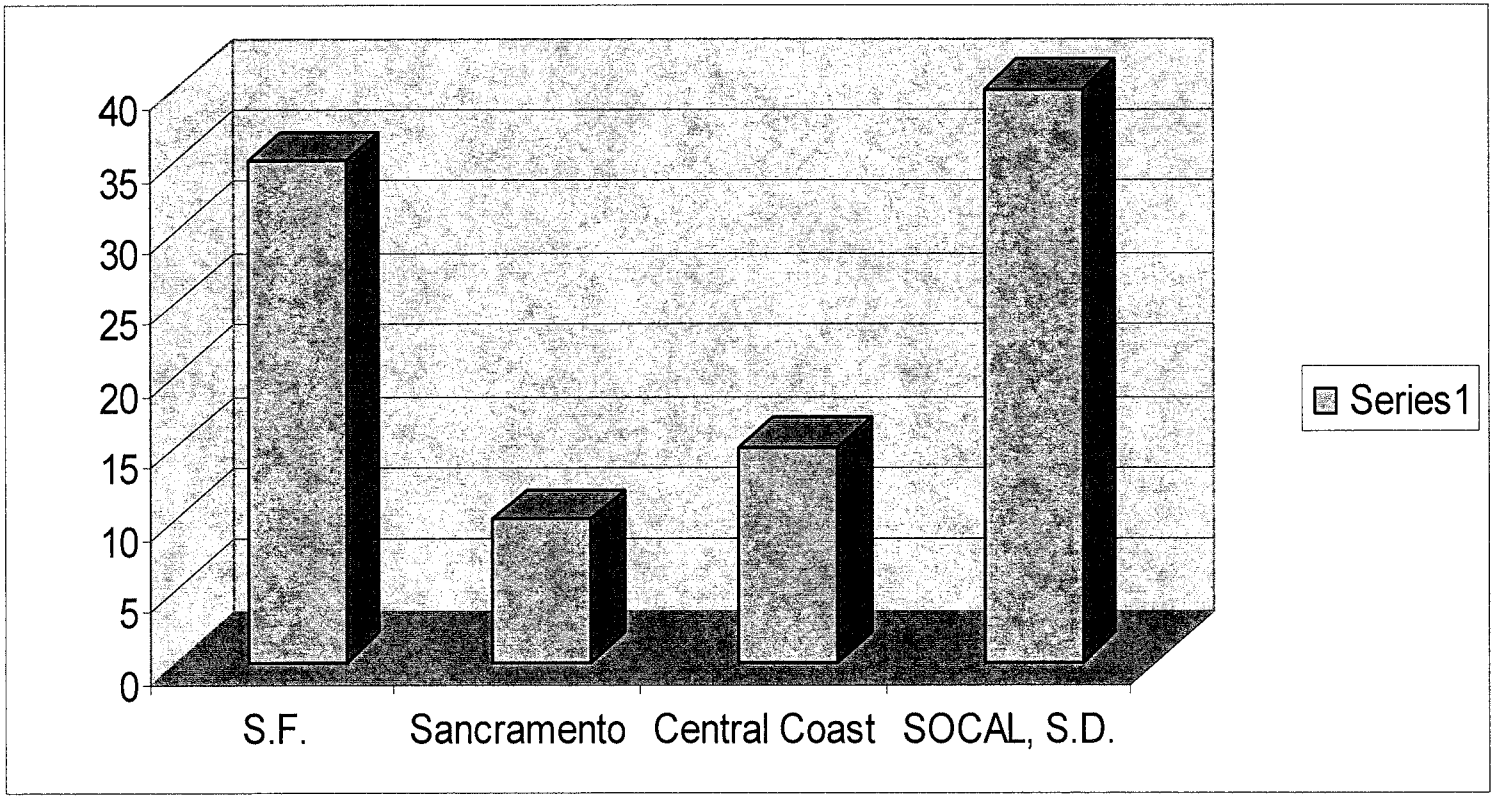
AB 2043 Port Security Respondent Organization

• Public port authority	41%
• Marine Terminal Facility Operator	21%
• Vessel Operator (Liquid Bulk)	4%
• Vessel Operator (Container)	4%
• Facility Operator (Container)	4%
• Facility Operator (Dry Bulk)	4%
• Facility Operator (Break-bulk)	4%
• Facility Operator (Chemical/Petroleum)	4%
• Ferry Operator	4%
• Other	10%

Respondent Trade/Distribution Lanes

• Cruise ship/passenger vessels	44%
• Ferry	32%
• Container	32%
• Neo-bulk (automobile/reefer)	25%
• Break-bulk	19%
• Liquid Bulk	25%
• Dry Bulk	32%
• Other	13%

Geographic representation:
35% San Francisco Bay area, 10% Sacramento, Stockton and Inland Rivers, Central coast 15%, Southern California Ventura –San Diego 40% adjusted



Adequate resources

(1) Federal government not doing enough in terms of resources and leadership to protect California's ports	
yes	56%
no	15%

Approved port security plan

(2) Have a USCG port security assessment in their port or facility	
yes	70%
no	30%

(3) Fifty-two per cent have participated in a USCG Area Security Plan	
yes	52%
no	48%

(4) Same percentage are required to have a maritime security plan under MTSA	
yes	52%
no	48%

Approved port security plan

(5) Same percentage have prepared a vulnerability assessment and facility security plan	
yes	72%
no	28%

(6) Have a pending or final USCG approved facility plan	65%
Have not submitted a plan for approval	20%

Major vulnerabilities or deficiencies

(7) Report no major vulnerabilities or deficiencies in the assessment and plan	**50%**
Report major vulnerabilities or deficiencies	**25%**
Don't know	**25%**

(8) Of those reporting major vulnerabilities, who reported landside and waterside perimeter security as significant	**80%**
Who had access control	**40%**
Who had each surface surveillance, effective counter-measures, security and non-security personnel training and awareness	**20%**

(9) Of those reporting major vulnerabilities or deficiencies	
Documented them	**40%**
Notified the appropriate regulatory agency	**20%**
Notified the corporate security officer	**20%**
Who had budgeted and taken corrective action from Federal sources by a 60 to 20 per cent margin.	**80%**

Port security grants

(10) Of port security grant applications	
Were for vulnerability assessments	26%
Were for perimeter security	47%
For access control	41%
For surveillance systems (CCTV, low light cameras, IR, motion sensors etc)	73%
For aerial surveillance and proof of concept, fixed or mobile command centers	7%
For non-intrusive examination technology	13%
Specialized security response equipment, training and support	13%
For drills and exercise participation, and contract physical security landside	20%
Waterside	7%

All Hazards Planning and Coordination

(11) Percent of the respondents report having an All Hazards Emergency Preparedness and Response Plan independent of their security plan	**60%**
Report a combined plan addressing all hazards and security incidents	**19%**

(12) Of those reporting an operationally integrated security plan with Federal, State or local government preparedness agency plans	
Yes	**40%**
No	**44%**

(13) Of the respondents have ongoing interaction with the USCG concerning their security plans including eleven per cent active teaming	**56%**
Jointly prepared planning	**11%**
Actively exercised plans	**45%**

(14) Of the respondents have ongoing discussions of their plans with the port authority	**13%**
Have teamed with them	**25%**
Have jointly prepared plans	**13%**
Have actively exercised plans	**50%**

(15) Of the respondents have ongoing discussions of their plans with the State Office of Emergency Services	**43%**
Have teamed with them	**15%**
Have actively exercised plans	**43%**

(16) Percent of respondents have ongoing discussions of their plans with the Governors Office of Homeland Security	**33%**
Have teamed with them	**17%**
Have actively exercised plans	**17%**

(17) Percent of respondents have ongoing discussions of their plans with the Federal Department of Homeland Security (DHS)	**43%**
Have teamed with them	**14%**
Have actively exercised plans	**14%**

(18) Percent of respondents have ongoing discussions of their plans with the Federal Emergency Management Agency (FEMA)	**33%**
Have teamed with them	**17%**
Have actively exercised plans	**17%**

(19) Percent of respondents have ongoing discussions of their plans with the Federal Transportation Security Administration (TSA)	**57%**
Have teamed with them	**15%**
Have actively exercised plans	**15%**

(20) Percent of the respondents have ongoing discussions of their plans with Local police, fire and other emergency responders	**38%**
Have teamed with them	**50%**
Have jointly prepared plans	**38%**
Have actively exercised plans	**50%**

(21) Percent of respondents have ongoing discussions of their plans with their counterpart facility or vessel operators	**33%**
Have teamed with them	**33%**
Have jointly prepared plans	**50%**
Have actively exercised plans	**50%**

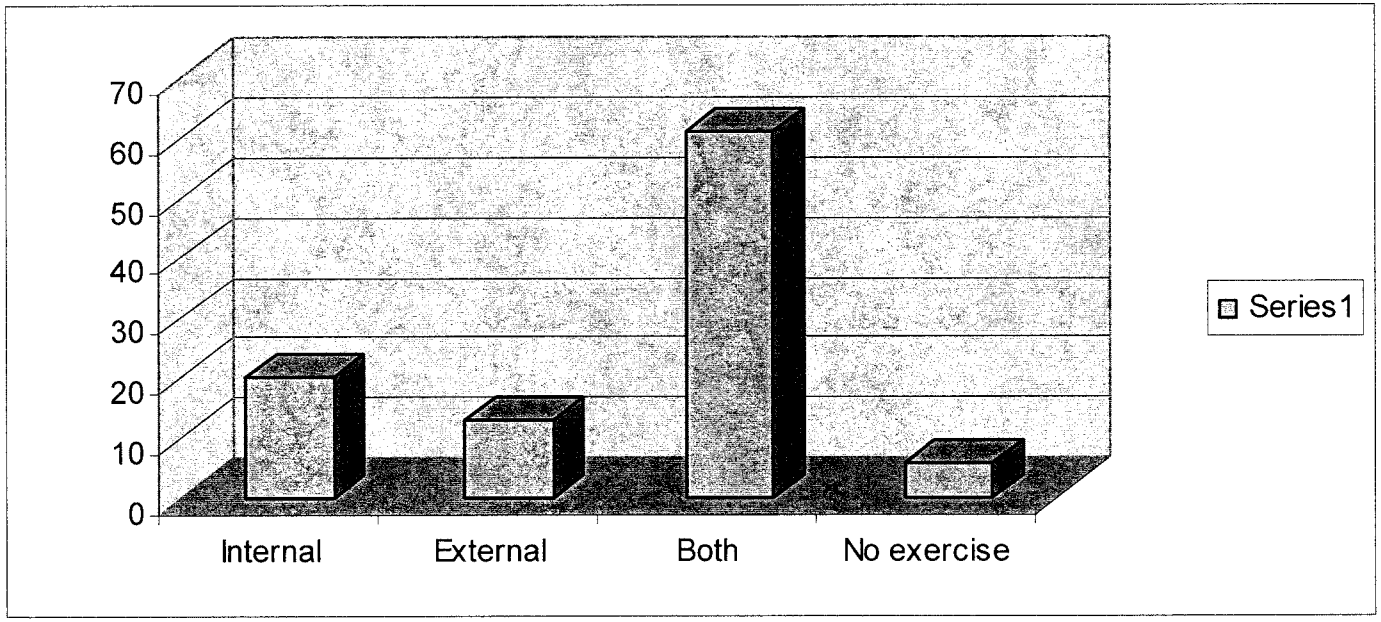
77

Port Security Plan Contents

(22) Mass casualty/medical response and triage	41%
Quarantine	14%
Mass Evacuation	50%
Operational coordination with Federal, State and local authorities	51%
Counter-terrorism	23%
WMD	29%
Natural disaster	89%
All of the above	10%

(23) All respondents conduct of table top or practice drills/exercises Monthly	4%
Quarterly	27%
Annually	40%
None	21%

(24) Exercise coordination:	41%
Internal	
External	14%
Both	50%
No exercise conduct	51%



(25) Compliance with required quarterly and annuals drills/exercises:	**4%**
In compliance	**27%**
No	**40%**
Uncertain	**21%**

80

Receipt of state pass-through port security grant assistance

(26) In 2004	
yes	11%
no	85%

(27) In 2005	
yes	22%
no	69%

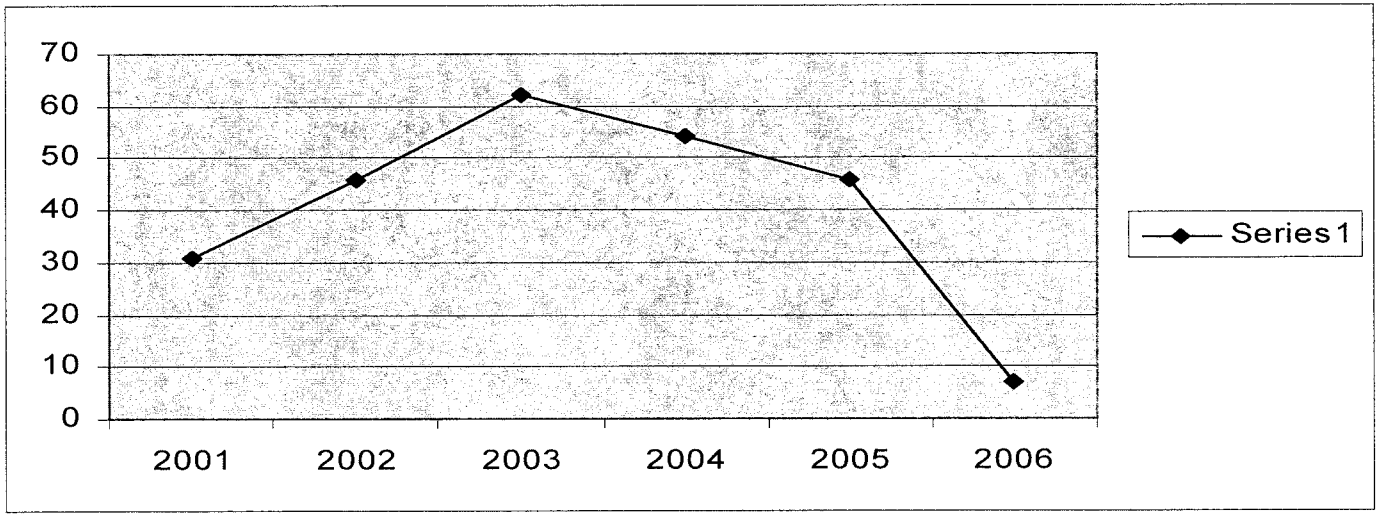
Uses of total port security grant funding

(28) Maritime domain awareness, WMD, counter-terrorism training	**0%**
Counter –terrorism first responder training	**6%**
Joint counter-terrorism training with first render network	**0%**
Joint port security-homeland security counter-terrorism exercise planning and conduct	**6%**
WMD and counter-terrorism response equipment	**6%**
None of the above	**80%**

(29) Public funds reserved for security personnel training and certification	
Yes	**0%**
no	**90%**

(30) Aggregate amounts of public funds received for port security purposes:	
<100k	29%
<250k	15%
<500k	7%
<1M	7%
<5M	7%
>5M	22%

(31) Years in which port security grants received:	
2001	31%
2002	46%
2003	62%
2004	54%
2005	46%
2006	7%



(32) Obligation of funds awarded:	
yes	50%
no	33%

(33) If fund not obligated reasons for:	
Internal organizational issues	33%
Matching or reimbursement requirements	0%
Contractor or vendor contracting delays	51%
Inability to locate qualified contractors	17%

(34) Coordination with another port, city, county, agency or other entity in port security grant application:	
yes	23%
no	65%

(35) Of those submitting, actually received grant involving multiple applicants:	
yes	15%
no	74%

Entity providing operational port security

(36) USCG	52%
DoD	0%
Harbor police	63%
Local municipality	26%
County Sheriff	21%
Private security company	42%
Fish and game authority	11%
Lifeguards	16%

Response equipment/capability

(37) Casualty vans:	
yes	5%
no	90%

(38) Vehicle staged on site	33%
Off site	33%
Uncertain	33%

(39) WMD event mass decontamination trailer, structure or facilities	
Yes	5%
No	85%

(40) Number of units:	
1 Unit	100%

(41) Throughput capacity: :	
1-5 persons per hour	100%

(42) On site explosive detection capability:	
yes	5%
no	90%

(43) Number of devices:	
2 – 5	100%

(44) Personnel protection equipment (e.g. bubble suits) to respond to HAZMAT incident:	
yes	11%
no	74%

(45) Number of response suits on site:	
2 – 5	100%

(46) Number of trained HAZMAT response personnel:	
2 – 5	50%
<10	50%

Emergency response time

(47) < 10 minutes	57%
10 – 30 minutes	15%
No answer	29%

Special needs agency designation

(48) DHS designation of CA as "Special Needs Agency" for port security grants like NYC"	
Yes	74%
no	11%

Establishment to CA Port security Emergency Preparedness Fund

(49) Establishment to CA Port security Emergency Preparedness Fund:	
yes	64%
no	5%
uncertain	26%

(50) Source of funds:	
Federal homeland security appropriations	84%
Federal user fees	50%
State General Fund homeland security appropriations	67%
State GO bonds	26%
State and local user fees	33%

Establishment to CA Port security Emergency Preparedness Fund

(51) Fund allocation:	
System wide assessment	27%
Area priority project list	16%
Local needs analysis and prioritization	32%
All of the above	58%

(52) Prioritization responsibility within organization:	
Port director	27%
Board of Commissioners	11%
Director of security	22%
Harbor police or equivalent	11%

Port and Intermodal Systems Center for Enhanced Security (PISCES)

(53) Favor participation in joint port security applied research projects:	
yes	90%
no	0%

Governor's Office of Homeland Security

(54) Permanent authority to administer Federal and State pass through grants:	
yes	31%
no	21%
uncertain	42%

Joint Harbor Operations Center

(55) Participation in JHOC:	
yes	32%
no	42%

Designation by Governor of statewide coordination office for port and marine transportation system issues

(56) yes	47%
no	16%
uncertain	32%

Naval Militia

(57) Support for establishment of naval militia as part of CA National Guard:	
yes	48%
no	31%
uncertain	21%

(58) Support for statewide bond measure to fund naval militia:	
yes	33%
no	67%

(59) Consistency of port security plan with Statewide All Hazards National Incident Management System (NIMS) Plan"	
yes	39%
no	55%

Continuity of operations/Consequence management

(60) Continuity of operations/consequence management plan:	
yes	32%
no	47%

(61) Updates to plan:	
Annually	46%
3 years	3%
5 years	23%

(62) Facility security plan integrate with consequence management plan:	
yes	57%
no	21%
uncertain	15%

(63) Planning, training and exercising basis:	
Worst case scenario	17%
Acceptable risk	39%
Uncertain	33%

(64) Planning considers major disruption or unavailability of key personnel:	
yes	42%
no	26%
uncertain	21%

(65) Planning considers operational capacity:	
yes	58%
no	21%
uncertain	11%

(66) Planning considers functional capability:	
yes	58%
no	16%
uncertain	16%

(67) Estimated down time to recover in event of major disruption:	
1-3 days	53%
4-7 days	1%
1 month	1%
uncertain	26%

(68) Average response time of security force to incident:	
<10 minutes	67%
<1 hour	2%
uncertain	17%

Continuity of Operation/Consequence Management

(69) Average Response Time for Key Management/Administrative personnel to incident:	
< 10 minutes	33%
< 1 hour	50%
< 2 hours	1%

(70) Average Response Time of operational personnel to incident :	
<10 minutes	44%
< 1 hour	39%
< 2 hours	6%

66

Continuity of Operation/Consequence Management

(71) Rating of overall readiness to detect, respond, and mitigate major security incident :	
Poorly prepared	17%
Adequately prepared	62%
Very well prepared	22%

(72) Facility security plan incorporate layered or zoned security to deter or delay intrusion:	
Yes	41%
No	35%
Uncertain	18%

100

Continuity of operation/Consequence Management

(73) Frequency of testing facility security plans :	
Weekly/Monthly	0%
Quarterly	39%
Semi-Annually/Annually	23%
Uncertain	22%
No testing	11%

(74) Adequacy of perimeter security (fencing, lighting, surveillance, monitoring, response, mitigation):	
Yes	23%
No	71%

Access Control

(75) Positive reliable verification of employees, contractors, vendors:	
Yes	67%
No	28%
Uncertain	5%

(76) Reliance solely upon primarily official or government or company issued photo identity:	
Yes	85%
No	8%

102

Port security training

(91) Training of employees to observe, detect, and report unusual behavior consistent with terrorist activity:	
yes	64%
no	5%
uncertain	26%

(92) Mandatory maritime security certification for employees :	
Yes	30%
Some	24%
None	12%
Not required	24%

Port security training

(93) Mandatory maritime security training for contractors and vendors:	
Some	18%
None	36%
Not required	30%

(94) Participation of senior management in port security training and certification:	
Yes	47%
No	41%
Uncertain	5%

Port Security training

(95) Company security officer experience level:	
1-2 yrs	0%
2-5 yrs	13%
5-10 yrs	13%
10-20 yrs	13%
>20 yrs	13%

(96) Facility security officer experience level:	
1-2 yrs	0%
2-5 yrs	6%
5-10 yrs	19%
10-20 yrs	25%
>20 yrs	13%

Port security training

(97) Facility security officer experience level:	
1-2 yrs	0%
2-5 yrs	6%
5-10 yrs	19%
10-20 yrs	25%
>20 yrs	13%

(98) Vessel security officer experience level:	
1-2 yrs	0%
2-5 yrs	7%
5-10 yrs	20%
10-20 yrs	0%
>20 yrs	13%

Port security training

(99) Area Maritime Security Committee/Harbor Safety Committee participation:	
Area/Harbor	**24%/ 18%**
Both	**41%**
Neither	**52%**
(100) Federal security clearance:	
Yes	**24%**
No	**59%**
(101) Coordination with Federal agencies in port security training:	
Yes	**53%**
No	**36%**
Uncertain	**12%**

Port security training

(102) Coordination with State agencies in port security training:	
Yes	30%
No	53%
Uncertain	18%

(103) Coordination with local agencies in port security training :	
Yes	65%
No	24%
Uncertain	12%
(104) Certification of staff members in HAZMAT response	
Yes	48%
No	30%
Uncertain	24%

Port security training

(105) Certification of staff members in emergency management and response:	50%
Yes	59%
No	24%
Uncertain	18%

(106) Certification of staff members in port security	
Yes	**42%**
No	**42%**
Uncertain	**18%**

Port security training

(107) Certification of staff members in maritime domain awareness:	
Yes	**24%**
No	**47%**
Uncertain	**30%**

(108) Certification of staff members in counter-terrorism response	
Yes	**18%**
No	**53%**
Uncertain	**30%**

110

Port security training

(109) Training funding sources	
Fee based	**50%**
No cost grant	**34%**

(110) Training scenarios reflect operational intelligence:	
Yes	**25%**
No	**47%**
Uncertain	**20%**

111

Port security training

(111) Port director, Commissioners, facility management involvement in port security training	
Yes	**50%**
No	**43%**
Uncertain	**8%**

(112) Type of port security training:	
Seminar	**31%**
Workshop	**31%**
Table top exercise	**77%**
Gaming/simulation	**15%**
Webcast/videoconfernce	**0%**
Field exercise	**31%**

112

Port security training

(113) Type of port security exercises:	
Seminar	**8%**
Workshop	**0%**
Table top exercise	**39%**
Gaming/simulation	**0%**
Webcast/videoconfernce	**0%**
Field exercise	**31%**

(114) Actual use of neutral evaluators (non-profit or academic) w/port security exercises:	
Yes	**29%**
No	**72%**

113

Port security training

(115) Potential use of neutral evaluators in port security exercises:	
Yes	**76%**
No	**22%**

(116) Potential use of regulatory "no fault"program:	
Yes	**75%**
No	**13%**
Uncertain	**13%**

Port security training

(117) Preparation of lessons learned after action reports:	
Yes	**69%**
No	**31%**

(118) Incorporation of lessons learned in training program:	
Yes	**92%**
No	**8%**

Port security training

(119) Sharing of lessons learned with other agencies:	
Yes	**46%**
No	**39%**
Uncertain	**15%**

(120) Reasons for not sharing lessons learned:	
Corporate policy	**50%**
Would share if practical and secure method available	**50%**

116

Port security training

(121) Administrative personnel participation in port security training:	
Yes	**29%**
No	**65%**
Uncertain	**7%**

(121) Operational and management personnel participation in port security training:	
Yes	**71%**
No	**21%**
Uncertain	**7%**

Port security training

(123) Emergency response personnel participation in port security training:	
Yes	**77%**
No	**23%**
Uncertain	**0%**
(124) Longshore, contractor, vendor personnel participation in port security training:	
Yes	**14%**
No	**86%**
Uncertain	**0%**

Port security training

(125) External first responder personnel participation in port security training	
Yes	**36%**
No	**64%**

(126) Participation with Federal agencies in port security exercises:	
Customs and Border Protection	**60%**
USCG	**80%**
TSA	**40%**
FBI	**60%**
DoD	**50%**

CTPATT, CSI, OSC participation

(127) CTPATT participation:	**29%**
CSI:	**14%**
ACE:	**29%**
ATS:	**43%**
NIE:	**43%**
Nuclear:	**57%**
Empty container inspection:	**43%**
(128) Of those reporting major vulnerabilities or deficiencies	
Documented them	**40%**
Notified the appropriate regulatory agency	**20%**
Notified the corporate security officer	**20%**
Who had budgeted and taken corrective action from Federal sources by a 60 to 20 per cent margin.	**80%**

Incident experience

(128) Alien smuggling	**50%**
Drug smuggling	**40%**
HAZMAT	**20%**
Major disruption	**30%**
Natural disaster	**70%**
Prolonged operational disruption	**20%**
Terrorist incident	**0%**
Terrorist surveillance	**10%**
Violent criminal incident	**10%**

Consequence management recovery capacity

(129) Auxiliary power generation	**70%**
Emergency food and water supply	**50%**
Cyber security	**90%**
Disaster mitigation	**90%**
Decontamination facility	**10%**
Medical mass casualty	**30%**
Damage control	**30%**
CBNRE mitigation	**0%**
Designated critical backup personnel	**0%**
Cross training critical functions	**3%**
Public relations plan	**90%**
Vessel and cargo diversion and routing plan	**10%**
Accelerated personnel replacement	**0%**
Continuity of operation plan	**30%**

Statewide clearinghouse for port security grants

(130) CA port security grant clearinghouse:	
Yes	**31%**
No	**15%**
Uncertain	**47%**

(131) Regional emergency operations centers participation	
Yes	**31%**
No	**39%**
Uncertain	**31%**

Red team test of port security plans

(132) Yes	**0%**
No	**93%**
Uncertain	**7%**

(133) Read team participation if services provided	
Yes if no cost	**91%**
Yes if subsidized rate	**17%**
Yes if reasonable user fee	**27%**

State responsibility for compliance with MTSA

(134) State concurrent responsibility Yes	**62%**
No	**15%**
Uncertain	**23%**

(135) State responsibility for port security training and exercises	
Yes	**61%**
No	**15%**
Uncertain	**23%**

State responsibility for MTSA compliance

(136) State responsibility for port police and other agencies maintaining effective counter-terrorism response capability Yes	**77%**
No	**15%**
Uncertain	**8%**

(137) State responsibility for seamless communication among first responders, law enforcement and port personnel	
Yes	**92%**
No	**8%**
(138) Comprehensive statewide port security plan	
Yes	**93%**
No	**7%**

Statewide port security plan

(138) Should goals of Statewide plan include vulnerability and threat assessment,risk mitigation, prevention and deterrence, emergency preparedness and response, and consequence management and recovery?	
Yes	**93%**
No	**7%**

CTPATT audit and Customs impacts	
(139) Experienced CTPATT audit	
Yes	**8%**
No	**85%**

(140) Increased post 9/11 cargo inspections	
Yes	**25%**
No	**42%**
Uncertain	**25%**

(141) Increased inspection related delays	
Yes	**25%**
No	**42%**
Uncertain	**25%**

Importance of port security foe cargo routing and port selection

(142) Importance of port security on cargo routing: Very important	**31%**
Somewhat important	**39%**
Not important	**15%**

(143) Impact of port security on logistic operations: Very significant	20%
Somewhat significant	**20%**
Insignificant	**30%**
No date to determine impact	**30%**

Supply chain impacts

(144) Supply chain delay due to port security: Very significant	**0%**
Somewhat significant	**30%**
Insignificant	**30%**
No data to determine impact	**30%**

(145) Additional cost of operations due to port security requirements: Very significant	0%
Somewhat significant	**20%**
Insignificant	**20%**

Supply chain impacts

(146) Increased contingency planning to prevent supply chain disruption: Yes	**11%**
No	**33%**
Uncertain	**22%**

(147) Importance of consequence management to port recovery: Very significant	37%
Somewhat significant	**27%**
Insignificant	**0%**
No data	**9%**

Improvements in CA port security since 9/11

(148) Significant increase in port security improvements	**27%**
Marginal increase	**36%**
No change	**18%**
No data	**18%**

(149) Change to threat level since 9/11: Significant increase	46%
Marginal increase	**9%**
Marginal decrease	**18%**
No data	**18%**

Adequacy of port security guidance and support from Federal, State and local officials

(150) Adequate support and leadership: Strongly agree	**0%**
Agree	**18%**
Barely adequate support	**18%**
Disagree	**27%**
Strongly disagree	**27%**
(151) Major areas in improvement for port security	
Better definition of regulatory requirements	**73%**
Closer cooperation and coordination among Federal, State and local agencies	**73%**
Uniform national standards and enforcement	**27%**
Uniform international standards and enforcement	**18%**
Better access to port security grant funding	**73%**
Better training and educational support	**82%**

Should We Fail to Protect Our Ports, What Consequences Should We Anticipate: Simulating the State-by-State Effects of Terrorist Attacks on Three Major U.S. Ports

Jiyoung Park, Prof. Peter Gordon, Prof. James E. Moore, II
and Prof. Harry W. Richardson

Center for Risk and Economic Analysis of Terrorism Events (CREATE)
University of Southern California

August 11, 2006

Securing California's Maritime Transportation System:
Seamless Operational Security (SOS)
Long Beach, CA

Contents

- Motivation
- Focus
- Modeling Process
- Data
- Model: Estimation of Trade Flows
- Model: Construction of NIEMO
- NIEMO Test
- Results
- Discussion

Motivation

Problems with available preliminary estimates of terrorist threat:

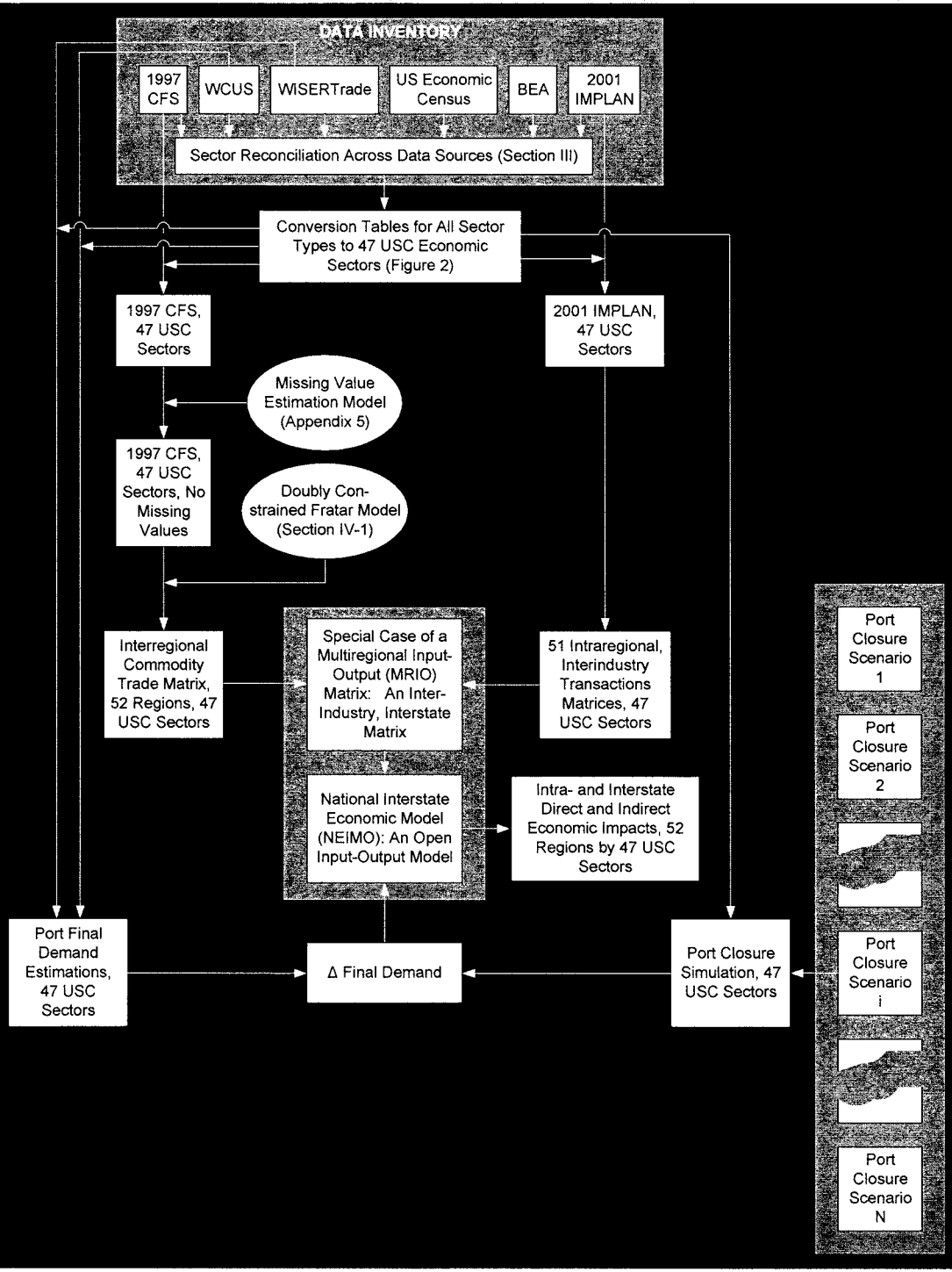
- The orders of magnitude are often much too vague to be useful ("millions of dollars," "up to billions of dollars," "a billion dollars a day").
- The estimates are too limited. There are many more than a dozen or so scenarios that pose a serious economic risk.
- The *incidence* of losses is not made clear. Decision makers have an interest in the spatial incidence of possible losses.

Focus

- Develop and test NIEMO (the National Interstate Economic Model).
- Apply NIEMO to simulate the economic impacts of terrorist attacks on any of 3 major U.S. seaports.

Modeling Process

Figure 1.
NIEMO Simulation Steps



CREATE, August 11, 2006

Data

Figure 2. Industrial Code Conversions (current $)

Sector System	USC	SCTG	BEA	NAICS	IMPLAN (2001)	SIC	HS	SITC	WCUS
USC									
SCTG	C, E								
BEA	C, E	C, E							
NAICS	C, E	C, E	A						
IMPLAN (2001)	C, E	C, E	A	A					
SIC	C, W	P	P	C, W	P				
HS	C, E	C, E	A	C, E	C, E	P			
SITC	C, W	C, W	P	P	P	P	C, W		
WCUS	C, W	C, W	P	P	P	P	C, W	C, E	

Notes:

***C*: Complete mapping**

A: Available from other sources

P: Possible to create mapping

E: Mappings constructed without any weights (Bayesian allocations)

W: Mappings constructed with plausible weights informed by additional data sources

Data (Continued)

Step 1-1	
IMPLAN (2001)	**BEA Code (1997)**
1. Industry.-to-Commodity. 2. One-to-One 3. Perfect 4. IMPLAN	

Step 1-2	
BEA code (1997)	**HS Code (1997)**
1. Commodity-to-Commodity. 2. One-to-Many 3. Very Good 4. BEA web	

Step 1-3	
HS Code (1997)	SCTG code (1997)
1. Commodity-to-Commodity 2. Many-to-One 3. Perfect 4. HS web	

Figure 3.
Data Reconciliation Steps, SCTG and IMPLAN

Step 2	
BEA Code (1997)	SCTG code (1997)
1. Commodity-to-Commodity 2. Almost Many-to- One 3. Very good	

Notes:
Bold: Used as Reconciliation Code
1: Sector type
2: One = One sector, Many = Multiple Sectors
3: Quality of Reconciled Data
4: Sources and Abbreviations:
IMPLAN
BEA: Bureau of Economic Analysis (http://www.bea.doc.gov)
SCTG : Standard Classification of Transported Goods (http://www.bts.gov/cfs/sctg/welcome.htm)
HS : Harmonized System (http://www.statcan.ca/trade/htdocs/hsinfo.html)

Step 3		
IMPLAN (2001)	**BEA Code (1997)**	SCTG code (1997)
1. Industry-to-Commodity 2. Almost Many-to-One 3. Very good		

Data (Continued)

- Data source reconciliation produces 47 USC Sectors, 29 of which are commodity sectors.
- Details are or will be available on the CREATE and METRANS websites.
  - http://www.usc.edu/dept/create/index.php
  - http://www.metrans.org/

Data (Continued)

Step 1-1	
USC Code	**HS Code**
1.Comm. to Comm. 2.One to Multi 3.Perfect 4.Created newly	

Step 1-2	
HS Code	**SITC Code**
1.Comm. to Comm. 2.Multi to one. 3.Very Good 4.WCUS, but revised	

Step 1-3	
SITC Code	WCUS Code
1.Comm. to Comm. 2.Multi. to One 3.Very Good 4.WCUS, but revised	

Data Reconciliation Process for NIEMO Tests

Step 2: Domestic Trade	
HS Code	WCUS Code
1.Comm. to Comm. 2.Almost Multi. to One 3.Very good	

Bold: Used as Bridge Code
1: Comm.= (Commodity)
2: One =One sector, Multi. =Sectors more than one
3: (Merged) Data Status
4: Source and Abbreviation
HS : Harmonized System (http://www.statcan.ca/trade/htdocs/hsinfo.html)
SITC: Standard International Trade Classification available from WISERTrade (http://www.wisertrade.org/home/index.jsp)
WCUS: Waterborne Commerce of the United States (http://www.iwr.usace.army.mil/ndc/data/datacomm.htm)

Step 3-1: Foreign Trade	
USC Code	SITG Code
1.Comm. to Comm. 2.Almost One to Multi 3.Very good	

Step 3-2: Domestic Trade	
USC Code	WCUS Code
1.Comm. to Comm. 2.Almost One to Multi 3.Very good	

Data (Continued)

Table 2. Top Ten U.S. Ports: Foreign Exports and Imports (Current $Millions, 2001)

2001 Rank	Ports	Exports	Ports	Imports
1	LOS ANGELES / LONG BEACH, CA	33,222	LOS ANGELES / LONG BEACH, CA	164,578
2	NEW YORK, NY / NEWARK, NJ	21,378	NEW YORK,NY / NEWARK, NJ	64,009
3	HOUSTON, TX	21,241	HOUSTON, TX	23,539
4	CHARLESTON, SC	12,836	SEATTLE, WA	23,209
5	NEW ORLEANS, LA	10,951	CHARLESTON, SC	20,876
6	NORFOLK, VA	10,892	OAKLAND, CA	16,021
7	OAKLAND, CA	9,194	BALTIMORE, D	15,686
8	MIAMI, FL	8,846	TACOMA, WA	13,943
9	SAVANNAH, GA	6,544	NORFOLK, VA	13,052
10	SEATTLE, WA	5,483	PHILADELPHIA, PA	11,877
	TOP TEN U.S. PORTS	140,587	TOP-TEN PORTS	366,790
	ALL U.S. PORTS	198,841	ALL U.S. PORTS	519,607
	TOTAL U.S. GOODS TRADE	718,762	TOTAL U.S. GOODS TRADE	1,145,927

Model: Estimation of Trade Flows

Estimating missing 1997 CFS data

- 1997 CFS includes unreported values for various commodities, including:
  - total shipments originating in some states
  - total shipments destined for some states
  - some trade flows between pairs of states
- An Adjusted Flow Model (AFM) is used to produce statistical estimates of missing 1997 values.

Model: Estimation of Trade Flows (Continued)

Updating 1997 data to estimates for 2001

- Based on 1997 trade tables completed via AFM, a Fratar model is used to estimate diagonal values for 2001.
- Traditional Fratar models are used to calibrate non-diagonal interregional cells given constraints on diagonal values.
- A Doubly-Constrained Fratar Model (DFM) estimates diagonal values and non-diagonal values simultaneously by combining new and traditional versions of the Fratar model.

Model: Construction of NIEMO

- Estimate Interstate Trade Flows for 2001 based on adjustments to the Commodity Flow Survey.
- Create 51 Inter-industry Input-Output Tables from 509 IMPLAN sectors, aggregating to 47 USC sectors.
  - 29 commodity sectors
  - 18 service sectors
- Invert a (52 x 47) x (52 x 47) matrix of technical and trade coefficients.

Model: Construction of NIEMO
(Continued)

Estimated Interstate Trade Flow Ratios: C matrix

		STATE1						...	STATE51						FOREIGN					
		I1	...	I29	I30	...	I47	...	I1	...	I29	I30	...	I47	I1	...	I29	I30	...	I47
STATE1	I1							...												
	...							...												
	I29							...												
	I30				1.0			...												
	...					1.0		...												
	I47						1.0	...												
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
STATE51	I1							...												
	...							...												
	I29							...												
	I30							...				1.0								
	...							...					1.0							
	I47							...						1.0						
FOREIGN	I1							...												
	...							...												
	I29							...												
	I30																			
	...																			
	I47																			

147

Model: Construction of NIEMO
(Continued)

Create 51 Inter-industry Input-Output Tables of Technical Coefficients from 509 IMPLAN sectors, aggregated to 47 USC sectors: **A** matrix

		STATE1						...	STATES1						FOREIGN					
		I1	...	I29	I30	...	I47	...	I1	...	I29	I30	...	I47	I1	...	I29	I30	...	I47
STATE1	I1							...												
	...							...												
	I29							...												
	I30							...												
	...							...												
	I47							...												
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
STATES1	I1							...												
	...							...												
	I29							...												
	I30							...												
	...							...												
	I47							...												
FOREIGN	I1							...												
	...							...												
	I29							...												
	I30							...												
	...							...												
	I47							...												

Model: Construction of NIEMO
(Continued)

Invert (52 x 47) x (52 x 47) matrix = $(I - C * A)^{-1}$

		STATE1						...	STATES1						FOREIGN					
		I1	...	I29	I30	...	I47	...	I1	...	I29	I30	...	I47	I1	...	I29	I30	...	I47
STATE1	I1							...												
								...												
	I29							...												
	I30																			
	...																			
	I47																			
...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...	...
STATES1	I1							...												
								...												
	I29							...												
	I30																			
	...																			
	I47																			
FOREIGN	I1							...							1.0					
								...								1.0				
	I29							...									1.0			
	I30																	1.0		
	...																		1.0	
	I47																			1.0

Tests

- We have compared results from simulations involving NIEMO and an aspatial IMPLAN model aggregated to 47 USC sectors.
- In the aggregate, the total output results for the two models differ by 0.92%.
- Sector-by-sector, most differences range from zero to 6%, tending toward the lower end of the range.
- Seven sectors showed differences greater than 10%.
- Some of the error is attributed to modeling a change in final demand change that is specific to just one state, California.

Results (Continued)

- Seaports Final Demand Estimations
  - LA/LB
  - Houston
  - NY/NW
- Terrorist Attack Simulations
  - Sum of Intra- and Inter-state Effects
  - Sectoral Effects

Results (Continued): Modeling Assumptions

- Loss of export opportunities trigger backward-linkage multiplier effects.
- Loss of import opportunities are less well modeled, and simply added as additional direct impacts.

Results (Continued):
Estimating One Month of Final Demand Associated with Each of Three Seaports

- Estimated Final Demand Losses, Port of Los Angeles/Long Beach Event: $4,115M in exports, 14,222M in imports
- Estimated Final Demand Losses, Port of Houston Event: $3,141M in exports, $3,219M in imports
- Estimated Final Demand Losses, Port of New York/Newark Event: $4,694M in exports, 6,700M in imports

Results (Continued) : Terrorist Attack Simulations

- Sum of Intra- and Inter-state Effects Associated with One-Month Shutdowns:
  - LA/LB $22,766M
    - Colorado $31.4M
    - Georgia $25.9M
  - NY/NJ $16,234M
    - Colorado $12.4M
    - Georgia $35.0M
  - Houston $ 9,733M
    - Colorado $21.9M
    - Georgia $23.6M

Results (Continued): Spatial Distribution of Economic Impacts by State, Port of Los Angeles and Long Beach Shut Down for One Month

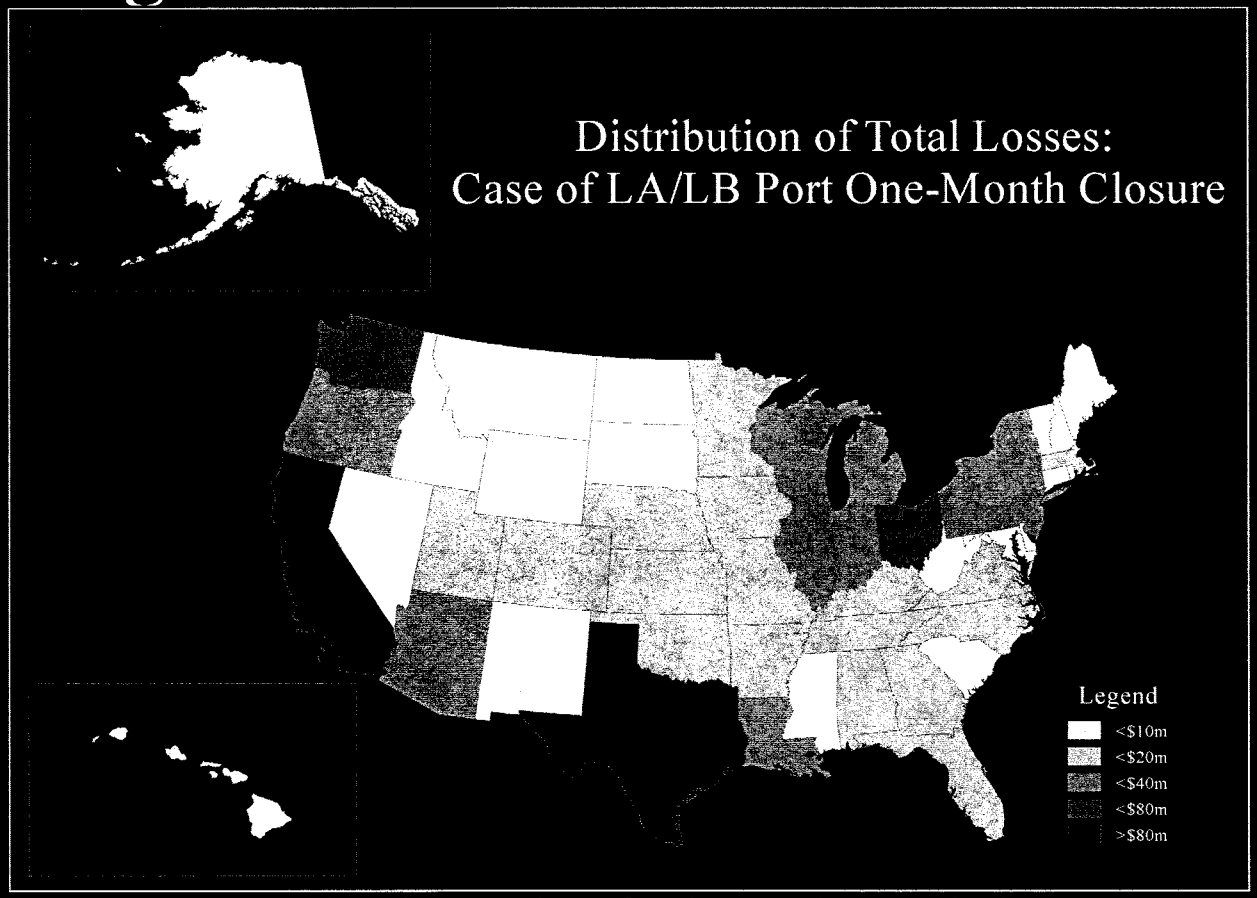


Figure 1.Distribution of Total Losses: Case of LA/LB Port One-Month Closure

Results (Continued) : Terrorist Attack Simulations

- USC Sector 24 (Electronic and Other Electrical Equipment) Effects Associated with One- Month Shutdowns:
  - LA/LB $ 3,997M
  - NY/NJ $ 933M
  - Houston $ 414M
- USC Sector 25 (Motorized Vehicles, Including Parts) Effects Associated with One- Month Shutdowns:
  - LA/LB $ 1,779M
  - NY/NJ $ 1,117M
  - Houston $ 241M

Results (Continued): Terrorist Attack Simulations

- USC Sector 10 (Coal and Petroleum Products) Impacts Associated with One- Month Shutdowns:
  - LA/LB $ 1,482M
  - NY/NJ $ 3,484M
  - Houston $ 1,994M
- USC Sector 29 (Miscellaneous Manufactured Products) Impacts Associated with One- Month Shutdowns:
  - LA/LB $ 1,312M
  - NY/NJ $ 560M
  - Houston $ 606M

Discussion

- As might be expected, state-by-state impacts are a function of size of state and distance from the attack.
- These are short-term impact analyses only.
- Demand-driven formulation does not adequately treat the economic constraints imposed by cessation of imports.
  - Supply-driven I/O models are controversial.
  - We are attempting to formulate a competing supply-driven formulation with the objective of reconciling use of both.
  - It may prove wisest to impose constraints on a demand-driven formulation.

Discussion (Continued)

- No induced effects via the household sector are measured.
- No substitution between ports is accounted for. A discrete choice model could account for choices between a fixed set of ports.
- These results provide a guide to the prioritization of port security expenditures.
- In a federal system, state-by-state impacts are useful for developing nationwide support for preventive investments at ports in distant states.

THE MARITIME INFRASTRUCTURE RECOVERY PLAN

FOR

THE NATIONAL STRATEGY FOR MARITIME SECURITY

APRIL 2006

FOREWORD

By signing National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD 41/HSPD 13), President Bush underscored the importance of securing the Maritime Domain, defined as *"All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances."*

NSPD 41/HSPD 13 established a Maritime Security Policy Coordinating Committee (MSPCC)—the first coordinating committee specifically tasked to address this issue—to oversee the development of a National Strategy for Maritime Security (NSMS) and eight supporting implementation plans:

- The **National Plan to Achieve Maritime Domain Awareness** lays the foundation for an effective understanding of anything associated with the Maritime Domain and identifying threats as early and as distant from our shores as possible.
- The **Global Maritime Intelligence Integration Plan** uses existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the Maritime Domain.
- The **Maritime Operational Threat Response Plan** aims for coordinated U.S. government response to threats against the U.S. and its interests in the Maritime Domain by establishing roles and responsibilities, which enable the government to respond quickly and decisively.
- The **International Outreach Strategy to Enhance Maritime Security** provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security.
- The **Maritime Infrastructure Recovery Plan** recommends standardized procedures for restoration of maritime transportation systems following an incident of national significance.
- The **Maritime Transportation Systems Security Plan** provides strategic recommendations to holistically improve the security of maritime transportation systems.
- The **Maritime Commerce Security Plan** establishes a comprehensive plan to secure the maritime supply chain.
- The **Domestic Outreach Plan** engages non-federal input to assist with the development and implementation of maritime security policies resulting from NSPD 41/HSPD 13.

Although these plans address different aspects of maritime security, they are mutually linked and reinforce each other. Together, NSMS and its supporting plans represent the beginning of a comprehensive national effort to promote global economic stability and protect legitimate activities, while preventing hostile or illegal acts within the Maritime Domain.

TABLE OF CONTENTS

I. INTRODUCTION TO THE MARITIME INFRASTRUCTURE RECOVERY PLAN

"A nation as vital and thriving as ours cannot become hermetically sealed. Even less can we afford to be overwhelmed by fear or paralyzed by the existence of threats. That's why we need to adopt a risk-based approach in both our operations and our philosophy. Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decision-making as we examine how we can best organize to prevent, respond and recover from an attack.... We all live with a certain amount of risk. That means that we tolerate that something bad can happen; we adjust our lives based on probability; and we take reasonable precautions."

DHS Secretary Chertoff
George Washington University
March 16, 2005

In addition to being an integral part of the HSPD-13 plans, the strategic guidance in the MIRP is reflected in the provisions of the National Maritime Security Plan (NMSP). The NMSP is a Maritime Transportation Security Act (MTSA) plan that addresses the restoration of domestic cargo flow following a security incident that occurs under, in, on, or adjacent to waters subject to the jurisdiction of the United States.

The Maritime Infrastructure Recovery Plan, the Maritime Commerce Security Plan, and the Maritime Transportation System Security Plan were developed in close coordination under the National Strategy for Maritime Security. The Maritime Commerce Security Plan contains recommendations to promote international maritime supply chain security and the Maritime Transportation System Security Plan addresses security of the Maritime Transportation System (MTS) as a system, including vessels, facilities, and ports. Both support the recovery of maritime capabilities.

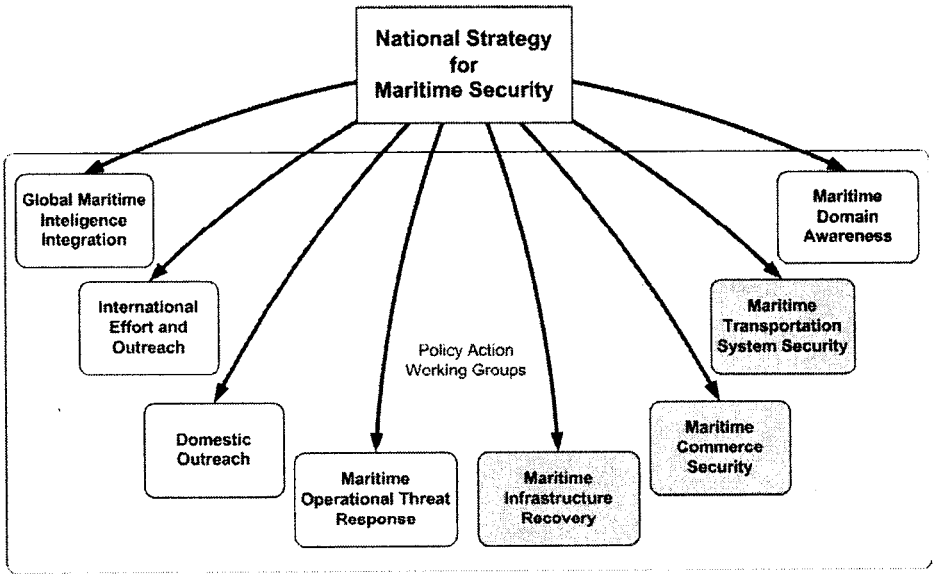


Figure 1.1 National Strategy for Maritime Security Policy Action Working Groups

The MIRP contains procedures for recovery management and provides mechanisms for national, regional, and local decision-makers to set priorities for redirecting commerce, a primary means of restoring domestic cargo flow. This plan is employed when the Secretary of Homeland Security declares an actual or threatened Transportation Security Incident (TSI; 33 CFR 101.105) that occurs under, in, on, or adjacent to waters subject to the jurisdiction of the United States, to be an Incident of National Significance (INS), in accordance with the criteria set out in the National Response Plan (NRP) and HSPD-5. Any such TSI declared to be an INS accordingly is referred to as a "national TSI."

Additionally, the MIRP reflects the organizational constructs detailed in the NRP, as well as the use of Incident Command System (ICS) and unified command procedures. As such, the plan can be used for other similarly disruptive incidents requiring maritime infrastructure recovery management.

Following an incident that triggers the implementation of this plan, the MIRP is used to guide the designees of the Secretary of Homeland Security in the decision making process to maintain the nation's MTS operational capabilities, and if compromised, to restore transportation capabilities.

In recognizing that recovery management takes place at several levels (i.e., national, regional, and local), the MIRP describes recovery management considerations for the incident site, non-incident support sites, as well as the national system-wide MTS. Decision-making affecting the nation's entire MTS draws on both domestic and international resources for recovery. The operational decisions to facilitate the diversion of cargo to alternate sites, including foreign ports, will be based on just-in-time information; currently there is no recognized methodology or uniform standards for measuring either domestic or foreign port cargo-handling capacity. Information of this type is necessary to support recovery efforts; however, it is not currently available. The need for port cargo-handling reserve capacity information is addressed in the Next Steps/ Recommendations Section of this plan.

Coincidental to operational considerations in recovery are those issues associated with the security posture necessary to re-establish any affected port to pre-incident equilibrium. Security postures are based on measured, targeted responses to ensure the public's well being and minimize disruption to the continuity of commerce. A basic assumption of the plan is that the MTS should not shut down as an automatic response to a maritime security incident.

Since this plan focuses on maritime transportation capabilities as a system, it only addresses the restoration of individual physical assets to restore the MTS. The vast majority of maritime transportation infrastructure assets are privately owned and operated. The decision to repair, replace, or rebuild private physical assets is a private sector decision. However, the federal government acknowledges that federal assistance may be required to help private industry in restoring critical cargo-handling infrastructure. Additionally, the plan recognizes that further study is needed to determine how the federal government can provide assistance or create incentives to private maritime stakeholders to establish sufficient critical cargo-handling infrastructure. (See Next Steps/Recommendations Section).

Since the MIRP provides recovery management procedures for decision makers at various levels, the procedures are general in nature to provide flexibility for recovery management. With over 2,100 possible threat scenarios in hundreds of ports, the variables affecting MTS recovery are too myriad to provide detailed procedures. Nevertheless, the procedures place emphasis on the importance of intelligence gathering and the use of risk management principles to make the decision-making considerations pertinent to any security-incident scenario. While the use of one particular risk-management model is not advocated, the plan strongly recommends that the recovery decision-making process involve personnel who have been trained in risk management/analysis so as to avoid uninformed decisions that would impose unnecessary constraints on the MTS. (See Next Steps/Recommendation Section about the need for risk management expertise.) The management of risk is also recognized in the Maritime Commerce Security Plan as being essential to balancing security with the desire to maintain the free flow of commerce. The Maritime Transportation System Security Plan recommends improvement of MTS security through the development of risk assessment methodologies. (See Appendix B for a description of Risk Management Principles).

In recognition that the federal government must work with private maritime stakeholders to restore passenger and cargo flow in an efficient manner, the plan encourages planning for recovery through development of private sector contingency/continuity of operations plans. The private sector is encouraged to develop recovery operations plans (within their business contingency plans) that include diversion of vessels to alternate ports and to engage in voluntary exchange of information with other companies to avoid conflicts in the use of alternate ports. (See the Roles and Responsibilities Section for the Private Sector).

The 9/11 Commission's report suggests the need for standards for private sector emergency preparedness and business continuity. In light of that identified need, this plan acknowledges that the federal government and the maritime private sector stakeholders should work together to plan for all aspects of recovery of the MTS after a security incident. The private sector is encouraged to collaborate with government and other stakeholders using professional organizations and Area Maritime Security (AMS) Committees. The Maritime Transportation System Security Plan suggests leveraging the value of AMS Committees by establishing threat response and recovery subcommittees and developing communications vehicles for use during normal and threat response/ recovery modes. There are many opportunities for communication and information sharing between government and the private sector; however, the MIRP recommends expanding the access to, and the capabilities of, one particular network in dealing with recovery activities (i.e. the Homeland Security Information Network (HSIN). (See Section IV – Concept of Operations as well as Next Steps/Recommendations about the communications network).

PURPOSE

The purpose of the MIRP is to establish a comprehensive approach to recover from a national TSI. As stated in the introductory portion of the plan, the focus of this plan is on maritime transportation capabilities (i.e., restoration of passenger and cargo flow) and minimizing impact of a security incident on the U.S. economy.

Assuming the effect of a national TSI (or other similarly disruptive incident) impairs the loading/offloading or movement of vessels, this plan provides a framework with clearly defined roles to facilitate restoration of cargo flow, as well as passenger vessel activity. Restoration of cargo flow and passenger vessel activity may include the redirecting/ diverting of vessels to ports with reserve or excess capacity.

To assist with the recovery/restoration of maritime transportation capabilities, the MIRP accomplishes or considers the following:

- Provides recovery management procedures for the Secretary of Homeland Security and designated representatives (e.g., the Interagency Incident Management Group (IIMG)) to make decisions affecting national maritime recovery efforts;
- Provides recovery management procedures for those making decisions at the incident site and at non-incident sites that provide support;
- Recognizes that, based on the nature and circumstances of the incident, a transition in focus from homeland defense operations to recovery management may occur between the Secretary of Defense and the Secretary of Homeland Security[1];
- Takes into consideration initial post-incident decisions made by senior officials from the U.S. Coast Guard (USCG) and the U.S. Customs and Border Protection (CBP) regarding short-term, targeted operational actions to help maintain flow of commerce through non-incident sites ;
- Lists roles and responsibilities of federal, state, local, tribal governments, and the private sector. The listing is specific to the functional responsibilities related to recovery of maritime transportation capabilities;
- To evaluate the effectiveness of the plan, the MIRP subscribes to an exercise program that includes periodic validation of the concepts of this recovery plan; and
- Identifies next steps and makes recommendations to improve recovery management.

OBJECTIVE

The primary objective of the MIRP is to provide guidance for federal decision makers to use in restoring maritime transportation capabilities if compromised, specifically the restoration of cargo flow and passenger vessel activity after a national TSI. This guidance includes recommended recovery management procedures to assist in the development of viable strategies or Courses of Action (COA).

To meet the primary objective stated above, a federal inter-agency working group was convened to develop a plan to satisfy the following functional planning objectives:

[1]During and following any homeland defense operations event, the Secretary of the Department of Homeland Security retains the lead for maritime infrastructure recovery management, and will ensure such activities align with homeland defense operations. Nothing in this plan will be construed to take precedence over homeland defense operations, including assignment of U.S. Coast Guard forces in accordance with current directives.

- Identify pre-designated key national government/industry stakeholders immediately available to advise the Secretary of Homeland Security on matters pertaining to recovery from INS affecting the Maritime Domain;
- Recommend national priorities for recovery of maritime transportation systems after a national TSI:
    - Define the criteria for identifying maritime critical infrastructure (MCI) across various maritime transportation subsystems;
    - Use Customs and Border Protection (CBP) inspection criteria for screening cargo to assist maritime recovery efforts and manage risk;
- Recommend federal policies and procedures for recovery of national maritime transportation after a security incident (and support recovery of critical local and regional transportation systems);
    - Establish standard procedures for setting decision-making priorities for recovery nationally, and for supporting recovery of critical local and regional transportation systems;
    - Set standard procedures for integrating national recovery priorities with national military requirements;
    - Maintain consistency with the National Response Plan (NRP);
    - Conduct a review of all legal authorities to ensure effective federal coordination of recovery and identify any recommend changes to eliminate statutory and regulatory gaps;
    - Establish standard procedures for assessing recovery requirements and developing potential recovery options within the Maritime Transportation System (MTS);
- Describe a maritime infrastructure recovery exercise program consistent with the National Exercise Program; and
- Specify procedures for coordinating among federal, state, local and private sector partners, and cooperation with foreign governments and international entities, as appropriate.

APPLICABILITY

Prior to declaration by the Secretary of Homeland Security that a TSI is an INS, response and recovery efforts are conducted under the purview and authority of Area Maritime Security (AMS) Plans in force for the affected geographic area, or Area of Responsibility (AOR), in which an incident has taken place.

When the Secretary of Homeland Security declares the TSI to be an Incident of National Significance ("national TSI"), decision-makers at the national level, as well as other levels, will address implications to the maritime industry nationwide, and will provide oversight to local and regional recovery operations utilizing the MIRP in conjunction with the National Maritime Security Plan (NMSP). The shift from local and regional to national incident management involves the activation of many plans. See the diagram in Section IV. Concept of Operations, for a graphic representation of the relationship of these plans.

AUTHORITIES

Various federal statutory authorities and policies provide the basis for federal actions and activities in the context of maritime infrastructure recovery. As described in the Foreword of this plan, the MIRP uses the foundation provided by the National Strategy for Maritime Security (NSMS) pursuant to the National Security Presidential Directive - 41/Homeland Security Presidential Directive - 13 (NSPD-41/HSPD-13) in conjunction with the National Maritime Security Plan to provide guidance for the restoration and recovery of cargo flow.

The MIRP does not in any way alter the existing authorities of individual federal departments and agencies. The MIRP does not convey new authorities upon the Secretary of Homeland Security or any other federal official. Rather, this plan establishes the coordinating structures, processes and protocols required to integrate specific statutory and policy authorities of various federal departments and agencies in a collective framework for action and activities to recover from a national TSI. All questions concerning specific authority and jurisdiction must be referred to competent counsel.

FEDERALISM

In regard to authority to preempt state action, when a Coast Guard official takes action pursuant to this plan, and that action implements or enforces an existing federal legal requirement for maritime security, it would be inconsistent with the Federalism principles set out in the Executive Order 13132 to construe that action as not preempting state laws or regulations that conflict with the existing federal legal requirement. This is because owners or operators of facilities or vessels, including those owned and operated by states, that may be subject to federal legal requirements for maritime security for both performance and operating standards, must have one uniform national standard that they must meet. Vessels and shipping companies, particularly, would be confronted with an unreasonable burden if they had to comply with varying requirements as they moved from state to state. Therefore, the Federalism principles enumerated by the Supreme Court in U.S. v. Locke, 529 U.S. 89 (2000) regarding field preemption of certain state vessel safety, equipment, and operating requirements extends to actions taken pursuant to this plan which implement or enforce an existing federal legal requirement for maritime security, especially regarding the longstanding history of significant Coast Guard maritime security regulation and control of vessels for security purposes. The same considerations apply to facilities, at least insofar as a state law or regulation applicable to the same subject for the purpose of protecting the security of the facility would conflict with a federal legal requirement; in other words, it would either actually conflict or would frustrate an overriding federal need for uniformity.

Finally, it is important to note that actions taken by the Coast Guard pursuant to this plan which implement or enforce an existing federal legal requirement for maritime security bear on national and international commerce, where there is no constitutional presumption of concurrent State regulation. Many aspects of federal legal requirements for maritime security are based on the U.S. international treaty obligations regarding vessel and port facility security contained in the International Convention for the Safety or Life at Sea, 1974, TIAS 9700; Rectification (1982), TIAS 10626, as amended, and the

complementary International Ship and Port Facility Security Code. These international obligations reinforce the need for uniformity regarding maritime commerce.

The authorities of federal agencies, other than the Coast Guard, may also preempt state action due a need to maintain national uniformity, to satisfy international obligations, to carry out express Congressional intent, to comply with specific case law, or due to a history of longstanding regulation. All questions concerning specific agency authority to preempt state action must be referred to competent counsel.

Notwithstanding the foregoing position, the federal government intends to consult with appropriate state officials and the private sector as set out in the plan.

DISCRETIONARY ENFORCEMENT

Following an incident that triggers the implementation of this plan, the MIRP anticipates that the private sector and appropriate federal government agencies will take actions that will result in large scale re-routing of vessel and cargo traffic. This re-routing will result in, among many other things, private sector requests for vessel, crew, and cargo clearances outside of normal lead times currently required by law. Further, re-routing of traffic and the need to move high priority cargo may result in the use of foreign registered platforms to carry cargo on coastwise voyages, and use of U.S. registered platforms to carry cargo on foreign voyages, or both, depending on the circumstances.

This plan does not change any authorities applicable to the aforementioned clearance processes or voyage routes. Federal agencies must be prepared to balance the continued need for security against the need to recover cargo flow to support the national economy. Accordingly, agencies should ease enforcement of laws regulating notices of arrival, crew and cargo manifests, and the coastwise trade, when such actions would enhance restoration of cargo flow without compromising security. Specifically, when re-routing of cargo results in changes only to destination and lead time of notice, and not to other required information such as cargo, vessel description and crew composition, agencies should be favorably disposed to approve such changes as soon as possible on an individual or company fleet-wide basis.

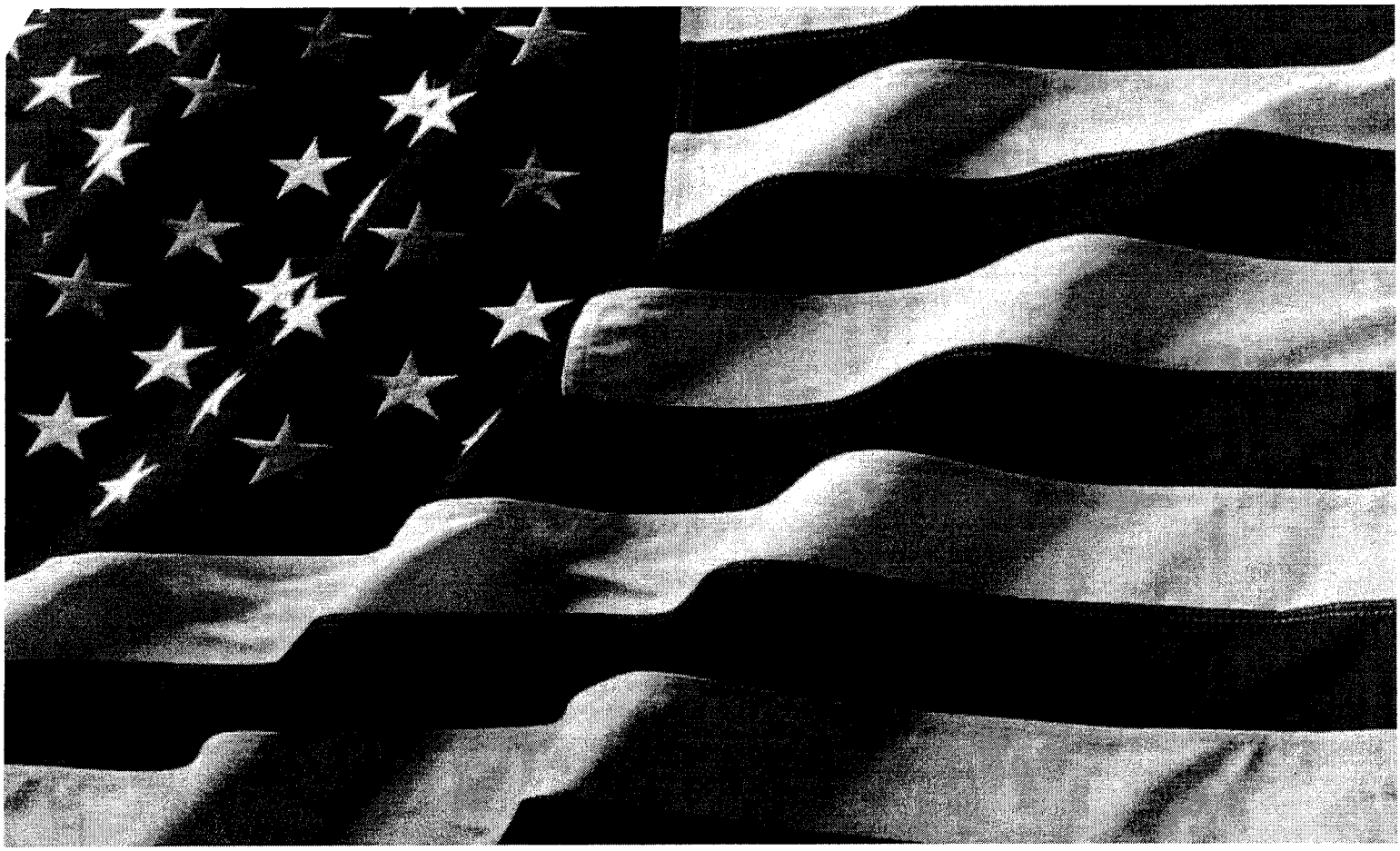
Agencies also must recognize that strict enforcement of coastwise trade regulations that results in a bar to employment of otherwise capable and secure platforms (U.S. or foreign registered) to move cargo to, from, or within the United States from foreign or domestic ports, may not be in the national interest. Accordingly, agencies should ease enforcement of coastwise trade regulations to ensure that all available platforms are readily available to move cargo to, from, or within the United States, from foreign or domestic ports, in the weeks following the incident, so that adverse economic impact is mitigated as soon as possible.

II. Planning Assumptions and Considerations

The Maritime Infrastructure Recovery Plan (MIRP) is based on the following planning assumptions and considerations:

- The MIRP is a guidance document used by incident managers, advisors, and decision makers;
- Implementation of the MIRP is based on the occurrence of a national TSI, which has been declared an INS by the Secretary of DHS, that has impaired or threatens to impair the loading/offloading or movement of vessels and disrupts the flow of commerce;
- This plan assumes that a national TSI has been declared, the National Response Plan (NRP), and its Interagency Incident Management Group (IIMG) has convened and is available to make national-level recommendations regarding the restoration of cargo flow and maritime infrastructure recovery;
- Recovery operations are based on risk management principles—100% security of the MTS cannot be guaranteed before or following an incident;
- The goals of decision makers utilizing the MIRP are:
    - Facilitate achieving the optimum balance between ports and waterways security and the recovery of maritime transportation capabilities,
    - Maximize the Maritime Transportation System's (MTS) continued operational equilibrium,
    - Minimize disruption to the U. S. economy from unnecessarily constrained cargo flow;
- Infrastructure refers to the Maritime Transportation System (MTS) and those facilities, structures, and assets vital to the Nation's ports (33 CFR 101.105);
- Use of the phrase "recovery or restoration of cargo flow" refers to recovery of goods, wares, and merchandise (33CFR 101.105) and restoration of maritime transportation capabilities in the MTS. Additionally, when referring to either recovery or restoration of cargo flow, the phrase includes recovery management associated with passenger vessel activity;
- The MIRP will be implemented with awareness of the initial measured and targeted response and recovery actions exercised by senior U.S. Coast Guard and Customs and Border Protection officials;
- A basic assumption of the plan is that the MTS should not be shut down as an automatic response to a maritime security incident;
- The plan includes next steps/recommendations to assess reserve or excess port-handling capacity at ports in North America (including both Canada and Mexico) and at other ports outside of North America. *The capacity of a port is the level at which the port can move cargo and passengers through the Maritime Transportation System, including the ability to safely and securely load and unload cargo and passengers and accommodate inter-modal operations*;
- "Minimizing damage (i.e., physical infrastructure damage) from attacks within the Maritime Domain" is covered under separate preparedness and incident response plans and, therefore, is not addressed in the MIRP;

- Key public and private maritime sector stakeholder inputs were considered in the development of the MIRP;
- Planners will consult with the private sector to update the MIRP to ensure meaningful, up-to-date decision-making information for federal officials; and
- Periodically, the MIRP will be updated as required to incorporate new Presidential Directives, legislative changes, and procedural changes based on lessons learned from exercises and actual events.



U.S. Department of Homeland Security

Office of Grants and Training

FY 2006 Infrastructure Grant Programs

Program Summary

Foreword

I am pleased to provide this summary of the FY 2006 program guidelines for the U.S. Department of Homeland Security Infrastructure Protection Grant Programs.

This is the first grant cycle since completion of the Department's Second Stage Review last summer and our creation of a unified Preparedness Directorate, which includes the essential work of the Office of Grants and Training. The preparedness mission is shared by the entire Department. Our approach to preparedness aggregates critical assets within DHS to support our operating components and the work of our external partners to prevent, protect against, respond to, and recover from threats to America's safety and security. The Directorate serves a strategic integration function of people, funding and programs.

In managing our grant programs, DHS is committed to supporting risk-based investments. We are equally committed to continuous innovation. As new infrastructure is built, existing facilities improved, or as our assessment of specific threats change, DHS grant programs will focus on being agile and making high-return investments to combat terrorism. The grant guidance for each of the individual FY2006 grant programs indicates the specific risk-based priorities that will drive DHS investments during the current grant cycle.

In 2006, $399 million is available for a series of related infrastructure protection grants. These grants programs are:

Port Security Grant Program: More than $168 million will be provided for port security grants to create sustainable, risk-based efforts for the protection of critical port infrastructure from terrorism. The Nation's 100 most critical seaports (plus an additional seaport eligible in 2005), representing 95 percent of the foreign waterborne commerce of the United States, are eligible to participate in the port grant program.

Transit Security Grant Program: Transit security grants are funded at more than $136 million this fiscal year for grants to the owners and operators of the nation's critical transit infrastructure including rail, intracity bus and ferry systems. Eligibility for funding is limited to those who provide services within a defined Urban Area Security Initiative (UASI) jurisdiction. A priority for this grant cycle is the protection of underground operations from improvised explosive devices.

Intercity Bus Security Grant Program: Approximately $9.5 million will be provided to eligible owners and operators of fixed route intercity and charter bus services to protect bus systems and the traveling public from terrorism. Program priorities include facility, driver and vehicle security enhancements; emergency communications technology; coordinating with local police and emergency responders; training and exercises; and passenger and baggage screening programs in defined UASI service areas.

Intercity Passenger Rail Security Grant Program: Amtrak will be awarded more than $7.2 million to continue security enhancements for intercity passenger rail operations in the Northeast Corridor (service between Washington, DC and Boston), Amtrak's hub in Chicago and expand these enhancements into the West Coast Service Area in key, high-risk urban areas.

Trucking Security Program: The American Trucking Association will receive $4.8 million for the Highway Watch program to continue to enhance security and overall preparedness on our nation's highways. The grant priorities of the Trucking Security Program include participant identification and recruitment; ensuring that the Highway Watch Program addresses homeland security and safety issues in conjunction with the National Preparedness Goal; and maintaining a full-time Highway Watch Call Center.

Buffer Zone Protection Program Grants: The Buffer Zone Protection Program provides grant funding to build security and risk-management capabilities to secure critical infrastructure including chemical facilities, nuclear and electric power plants, dams, stadiums, arenas and other high-risk areas. In FY06, this program will award approximately $48 million in grant funds to state and local authorities.

Chemical Sector Buffer Zone Protection Grant Program: The Chemical Sector Buffer Zone Protection Grant Program is a targeted effort that provides funds to build security and risk-management capabilities at the state and local level for chemical sector critical infrastructure from acts of terror and other hazards. In FY06, the Chemical Buffer Zone Protection Program will receive $25 million.

For each grant, the Preparedness Directorate will rely on an integrated team of subject matter experts drawn from both DHS operating components and sector specific Departments to develop, design, compete, review, and support the infrastructure grants as part of the national preparedness effort.

DHS is committed to working with the owners and operators of America's critical infrastructure as part of the national effort to reduce the risks from terrorism and other threats to the homeland.

Michael Chertoff
Secretary
Department of Homeland Security

Note

This summary document of the FY 2006 infrastructure protection grant programs does not constitute nor substitute for grant guidance. Detailed guidance and grant application information are contained in the individual grant program packages available at www.grants.gov. This summary is intended for information purposes only as a convenient compendium of the infrastructure protection grant programs of the Department of Homeland Security.

Contents

FY 2006 Port Security Grant Program (PSGP)

Purpose

The purpose of the FY 2006 PSGP is to create a sustainable, risk-based effort for the protection of critical port infrastructure from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

The FY 2006 PSGP also seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goal and the associated National Priorities. Through its focus on port-wide risk management planning, improvised explosive devices, non-conventional methods of attack and domain awareness in the port environment, the FY 2006 PSGP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System and the National Response Plan;
3. Implementing the National Infrastructure Protection Plan;
4. Strengthening information sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and,
6. Strengthening chemical, biological, radiological, nuclear and explosive detection and response capabilities.

In addition, the FY 2006 PSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the port environment.

Funding

Funding is **$168,052,500** for port security grants. Funding will be provided directly to successful applicants.

Public sector applicants must provide matching funds supporting **at least 25 percent of the total project cost** for each proposed project. **Private sector** applicants must provide matching funds supporting **at least 50 percent of the total project cost** for each proposed project.

Solicitation

The FY 2006 Port Security Grant Program is the sixth round of grants and builds upon the previous five rounds. Successful applications will be selected by a competitive process. Eligible applicants in each port area may submit one application for funding of up to five (5) individual projects.[1] Funding may be awarded for all, some or none of the projects submitted based on the outcome of the evaluation process.

[1] An individual project could be a single activity or multiple activities required to complete an action, such as the establishment of a canine program or an enhanced employee identification system. Individual projects must take place at a single port area.

Project Selection

A series of reviews will be conducted by local and national subject matter experts to ensure the most effective distribution of funding among these ports. Awards under this program will not be based on formula distributions, but rather on risk-based analytical assessments that align with the program goals outlined in the full grant application package.

In order to assure that port areas are competing for funds on an equal footing with port areas with similar risk ratings, each port area will be sorted by risk into tiers. Each tier will be given a specific allotment of grant funds for which port areas will compete. *Consequently, applicants will compete for funding against only those port areas with similar risk rankings.*

The series of reviews are:

1. **Initial Screening.** DHS Office of Grants and Training (G&T) staff will receive and conduct an initial review of all FY 2006 PSGP applications.

2. **Field Review.** Field level reviews will be managed by the applicable United States Coast Guard (USCG) Captain of the Port (COTP) in coordination with the Maritime Administration (MARAD) Regional Director and appropriate personnel from the Area Maritime Security Committee and/or local law enforcement (as identified by the COTP). For each port, the COTP will submit to DHS evaluations that include the following: (1) each specific application will be scored for compliance with the four core grant program criteria enumerated below, and a total score will be computed; and (2) all proposals received from each port will be rank ordered from highest to lowest in terms of their contributions to risk reduction and cost effectiveness. The four core PSGP criteria are as follows:

   - *Criteria #1.* Projects that support the national port security priorities:
     - Prevention and detection of Improvised Explosive Device (IED) attacks by small craft;
     - Prevention and detection of vehicle-borne IEDs on ferries;
     - Prevention and detection of underwater IED attacks; and,
     - Enhancement of the port area's Maritime Domain Awareness (e.g., access control/standardized credentialing, command and control, communications and enhanced intelligence sharing and analysis);
   - *Criteria #2.* Projects that address priorities outlined in the applicable Area Maritime Security Plan;
   - *Criteria #3.* Projects that address additional security priorities based on the COTP's expertise and experience with the specific port area; and,
   - *Criteria #4.* Projects that offer the highest potential for risk reduction for the least cost.

Projects will be rated against the above noted program criteria. The COTP will score specific applications on a four-point scale, and scores will reflect responsiveness to the four core criteria.

After completing field reviews, the COTPs will submit prioritized listings of projects for each port area to USCG District staff to ensure consistent application of field review guidance. After review by USCG District staff, COTPs will then submit the field review prioritized lists to G&T to begin coordination of the national review process.

3. **National Review.** Following the field review, a National Review Panel will be convened. The panel will include subject matter experts from USCG, Transportation Security Administration (TSA), Customs and Border Patrol (CBP), Office of Infrastructure Protection (IP), MARAD, and G&T. The purpose of the National Review Process is to identify a final, prioritized list of projects for funding.

Eligibility

The Nation's 100 most critical seaports[2], representing 95 percent of the foreign waterborne commerce of the United States, plus an additional port area eligible in FY 2005, have been identified for inclusion in the FY 2006 PSGP. Eligible facilities within these port areas must be within two miles of the commercial waterway. Additionally, if a facility falls outside the recognized boundaries of one of these port areas, but is addressed in the port's Area Maritime Security Plan, it will be considered eligible. **Presence on the FY 2006 PSGP eligibility list does not guarantee funding.**

Within the eligible port areas, applicants must be:

- Owners/operators of federally regulated public or private ports, terminals, U.S. inspected passenger vessels, or ferries as defined in 33 CFR Parts 101, 104, and 105;
- Port authorities, and/or State and local agencies that provide layered security protection to federally regulated facilities; or,
- Consortia composed of local stakeholder groups (i.e. river groups, ports, and terminal associations) representing federally regulated ports, terminals, U.S. inspected passenger vessels, or ferries.

[2] The Port Criticality List was developed by the U.S. Coast Guard using commercial, demographic and geographic data from various sources. Factors such as Cargo Volume and Passenger Volume, the presence of Critical Infrastructure/Key Assets (CI/KA), and Strategic Importance, among others, were used in the determination. Its purpose is to identify ports that are essential to the viability of the Marine Transportation System. Ports on this list represent 95 percent of the foreign waterborne commerce of the United States.

FY 2006 PSGP Eligible Port Areas

Port Areas	
Albany, NY	Nashville, TN
Anacortes, WA	New Haven, CT
Anchorage, AK	New London, CT
Baltimore, MD	New Orleans, LA
Baton Rouge, LA	New York/New Jersey
Beaumont, TX	Newport News, VA
Boston, MA	Norfolk Harbor, VA
Bridgeport, CT	Oakland, CA
Brownsville, TX	Palm Beach, FL
Buffalo, NY	Panama City, FL
Burns Harbor, IN	Pascagoula, MS
Camden, NJ	Paulsboro, NJ
Charleston, SC	Penn Manor, PA
Chattanooga, TN	Pensacola, FL
Chester, PA	Philadelphia, PA
Chicago, IL	Pittsburgh, PA
Cincinnati, OH	Plaquemines, LA
Cleveland, OH	Ponce, PR
Corpus Christi, TX	Port Arthur, TX
Detroit, MI	Port Canaveral, FL
Duluth-Superior, MN/WI	Port Everglades, FL
Everett, WA	Port Hueneme, CA
Freeport, TX	Port Manatee, FL
Galveston, TX	Port St. Joe, FL
Gary, IN	Portland, ME
Green Bay, WI	Portland, OR
Greenville, MS	Portsmouth, NH
Gulfport, MS	Providence, RI
Guntersville, AL	Richmond, CA
Helena, AR	San Diego, CA
Honolulu, HI	San Francisco, CA
Houston, TX	San Juan, PR
Huntington, WV	Savannah, GA
Indiana Harbor, IN	Seattle, WA
Jacksonville, FL	South Louisiana, LA
Kalama, WA	St. Louis, MO
Kansas City, MO	St. Paul, MN
Lake Charles, LA	Stockton, CA
Long Beach, CA	Tacoma, WA
Longview, WA	Tampa, FL
Los Angeles, CA	Texas City, TX
Louisville, KY	Toledo, OH
Marcus Hook, NJ	Tulsa, OK
Matagorda, TX	Two Harbors, MN
Memphis, TN	Valdez, AK
Miami, FL	Vancouver, WA
Milwaukee, WI	Vicksburg, MS
Minneapolis, MN	Victoria, TX
Mobile, AL	Wilmington, DE
Morehead City, NC	Wilmington, NC
Mount Vernon, IN	

Program Coordination

In developing the FY 2006 PSGP guidance, DHS coordinated with the following entities:

- *Department of Homeland Security:* Office of Grants and Training; United States Coast Guard; Transportation Security Administration; Office of Infrastructure Protection; Office of the Chief Intelligence Officer
- *Department of Transportation*: Maritime Administration
- *Industry:* American Association of Port Authorities; Port Security Council; various individual port and port facility operators and owners

This grant program was also informed by ongoing discussions with State and local law enforcement officials regarding infrastructure protection priorities.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Port Security Grant Program are available at the following web link: www.grants.gov.

FY 2006 Transit Security Grant Program (TSGP)

Purpose

The purpose of the FY 2006 Transit Security Grant Program is to create a sustainable, risk-based effort for the protection of critical transit infrastructure from terrorism, especially explosives and non-conventional threats that would cause major disruption to commerce and significant loss of life.

The FY 2006 TSGP also seeks to assist the Nation's transit systems in obtaining the resources required to support the Goal and the associated National Priorities. The program seeks to make risk-based investments focused on regional planning, infrastructure protection, improvised explosive devices (IEDs) and other non-conventional methods of attack, as well as training, exercises and citizen preparedness. The FY 2006 TSGP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System and the National Response Plan;
3. Implementing the National Infrastructure Protection Plan;
4. Strengthening information sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and,
6. Strengthening chemical, biological, radiological, nuclear and explosive detection and response capabilities.

In addition, the FY 2006 TSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the transit sector.

Funding

Funding totals **$136,045,000** for grants to the owners and operators of some of the Nation's most critical transit infrastructure, including heavy, light, and commuter rail, intracity bus and ferry systems. The Tier I and II structure used in the following table is explained below in the Project Selection section. In essence, Tier I funding is allocated to specific systems based upon risk and Tier II funding is allocated based upon risk-based competitive grants. All Ferry grants are allocated to specific systems based upon risk. The table below summarizes total program funding for this year's transit programs.

FY 2006 TSGP Funding by Mode

Transportation Mode	Funding
Rail Transit *(Tier I)*	$103M
Rail Transit *(Tier II)*	$7M
Intracity Bus *(Tier I)*	$15M
Intracity Bus *(Tier II)*	$6M
Ferry	$5M

Solicitation

Equipment acquisitions, drills and exercises, employee training programs, and public awareness programs that focus on mitigating the risk priorities represent appropriate use of TSGP funding.

Rail. The following rail specific risk-based priorities should be addressed for rail-related grants (as applicable):

1. Protection of underwater and other deep bore tunnels and associated track mileage from attacks employing IEDs;
2. Development and enhancement of capabilities to prevent, detect, and respond to terrorist attacks employing improvised explosive devices on other transit assets including stations, yards, and trains; and,
3. Mitigation of other high consequence risks identified through individual transit system risk assessments.

Bus. The following bus specific risk-based priorities should be addressed for bus-related grants (as applicable):

1. Development and enhancement of capabilities to improve inventory control, such as ignition key-recognition systems and remote tracking/shut-down capabilities. The use of intracity buses as a weapon poses a threat of great concern to intracity bus systems and critical infrastructure;
2. Increased perimeter security at intracity bus depots and yards. Related to the first priority, access control at areas of storage is an effective way to deter the use of intracity buses as a vehicle borne IED (VBIED);
3. Development and enhancement of training and awareness among intracity bus operators and employees;
4. Development of emergency response and preparedness capabilities in the event an intracity bus used as a weapon to inflict damage on critical infrastructure;

5. Implementation of technology-driven surveillance (e.g., CCTV), either at intracity bus facilities or within the buses, that can increase the effectiveness of other detection and deterrence measures; and,
6. Suspicious activity detection and behavior pattern recognition.

Ferry. The following ferry specific risk-based priorities should be addressed for ferry-related grants (as applicable):

1. Development and enhancement of capabilities to prevent, detect, and respond to terrorist attacks employing IEDs and VBIEDs;
2. Mitigation of other high consequence risks identified through individual ferry system risk assessments;
3. Use of canine teams at the embarkation and exit points of a system as well as during passage;
4. Innovative utilization of mobile technology for prevention and detection of explosives or other threats and hazards. This may include implementation of technology-driven surveillance (e.g., CCTV);
5. Development and enhancement of physical and perimeter security capabilities to deny access around maintenance facilities, dry docks, and piers;
6. Development and enhancement of training and awareness among ferry operators and employees. Training and awareness should cover the detection and deterrence of efforts by terrorists to use ferries as a means to attack critical infrastructure and key resources;
7. Development of emergency response and preparedness capabilities or drills in the event of a ferry being used as a weapon to inflict damage on critical infrastructure (e.g., nearby LNG terminals or vital cargo shipping lanes); and,
8. Citizen awareness training.

The U.S. Department of Transportation's Federal Transit Administration (FTA) has established 20 security program action items for transit system security readiness. Implementation of these action items enhances security posture generally and supports achievement of the National Preparedness Goal and national and regional strategies to mitigate risk. Eligible applicants are encouraged to review these action items and adopt those currently missing from their security program.

Project Selection

The FY 2006 TSGP will use risk-based prioritization consistent with DHS policy. As described above, the total amount of available transit grant funding was first allocated by transportation mode: rail, bus, and ferry. Next, risk-based project selection criteria priorities – based upon DHS analysis of consequences, vulnerability and threat for individual systems – were established using a two-tiered approach. For the highest-risk systems, a maximum amount of funding was established for specific systems, with distribution of funds subject to

approval by DHS of qualified projects (the Tier I grants). In the case of intracity rail and bus systems, DHS also created a pool of funds that will be awarded on a competitive basis to eligible systems that submit the best risk-based and cost-effective applications (the Tier II grants). All of the available ferry grant funds will be based on individual system allocations (i.e., as Tier I grants).

The Tier I transit regions or systems will have 90 days after the release of the grant guidance to submit detailed project plans to TSA for approval. Systems in the first tier may submit project plans as either regions or individual agencies. However, evidence of regional coordination and harmonization will be required. First tier rail, bus, and ferry regions are identified in the tables below in bold and with their proposed funding allocation listed. Project plans for Tier I systems will be evaluated on the following factors:

- Ability to reduce risk of catastrophic events;
- Overall effect on regional transit security;
- Cost effectiveness to include leveraging additional resources; and,
- Ability to complete the proposed project within the proposed timeframes.

Grants for both rail and bus Tier II systems will be competitively awarded based on the following factors:

- Ability to reduce risk;
- Cost effectiveness, to include leveraging additional resources; and,
- Ability to complete the proposed project within the timeframes.

The following method of selection will be used to evaluate Tier II system projects:

1. Rail and Bus agencies will submit concept papers for consideration. These concept papers will be submitted through www.grants.gov.
2. Concept papers will be reviewed and scored by a Federal Interagency Working Group consisting of TSA, FTA, and G&T;
3. Projects that are accepted will be required to complete full project applications;
4. G&T will verify compliance with each of the administrative and eligibility criteria identified in the application kit;
5. TSA will review the Federal Interagency Working Group recommendations and make recommendations for funding to G&T and the Secretary. TSA will brief all appropriate agencies on the final selections to ensure agreement for each grant work plan.

A Tier II grant applicant must be able to convey an understanding of the security priorities established under the TSGP guidance. At a minimum, each concept paper must:

- Define the vision, goals and objectives for the risk reduction the respondent is ultimately trying to achieve and how the proposed project will fit into an overall effort to meet critical infrastructure security priorities, including integration into existing security protocols;
- Describe the specific needs and/or resource limitations that need to be addressed;
- Identify any potential partners and their roles and staffing requirements, and provide information on any existing agreements such as Memorandums of Understanding (MOU);
- Propose a detailed budget and timeline; and,
- Adhere to a maximum limit of five pages.

In considering project plans for Tier I submissions, and concept papers for Tier II submissions, preference in awarding grants will be given to regions and agencies that propose providing matching funds or operations assets. DHS plans to implement matching grant criteria, similar to the port security program, for all FY 2007 transit grants.

Eligibility

Eligibility for intracity rail, intracity bus, and ferry grants under the 2006 TSGP for specific regions and transit systems was established based upon risk-analysis criteria developed at DHS, based upon inputs from our Federal, State, local, and industry partners. The eligible regions and systems for these grants are identified in the following three tables.

In the case of Tier I eligible awardees, the maximum possible funding is identified by dollar amount. All Tier II eligible awardees may compete for awards. The total pool of funds for Tier II awards will be: rail, $7 million; and bus, $6 million.

FY 2006 TSGP Eligible Rail Transit Systems

State	Urban Area	Regional Allocation/Eligibility	Eligible System	Eligible Mode
CA	**Bay Area**	**Tier I - $8.4M**	Peninsula Corridor Joint Powers Board	Commuter Rail
			San Francisco Bay Area Rapid Transit District	Heavy Rail
			Altamont Commuter Express	Commuter Rail
			Santa Clara Valley Transportation Authority	Light Rail
			San Francisco Municipal Railway	Commuter Rail, Light Rail
	Greater Los Angeles Area (Los Angeles/Long Beach and Anaheim/Santa Ana UASI Areas)	**Tier I - $4.0M**	Southern California Regional Rail Authority (Metrolink)	Commuter Rail
			Los Angeles County Metro Transportation Authority	Heavy Rail, Light Rail
	Sacramento	Tier II	Sacramento Regional Transit District	Light Rail
	San Diego	Tier II	North San Diego County Transit District	Commuter Rail
			San Diego Trolley, Inc.	Light Rail
CO	Denver	Tier II	Denver Regional Transportation District	Light Rail
DC/MD/VA[3]	**Greater National Capital Region (NCR and Baltimore UASI Areas)**	**Tier I - $13.0M**	Washington Metropolitan Area Transit Authority	Heavy Rail
			Virginia Railway Express	Commuter Rail
			Maryland Transit Administration	Commuter Rail, Heavy Rail, Light Rail
FL	Jacksonville	Tier II	Jacksonville Transportation Authority	Other Rail (AG)
	Miami/Fort Lauderdale	Tier II	Tri-County Commuter Rail	Commuter Rail
			Miami-Dade Transit	Heavy Rail, Other Rail (AG)
GA	**Atlanta**	Tier I - **$2.0M**	Metropolitan Atlanta Rapid Transit Authority	Heavy Rail
IL/IN[4]	**Chicago**	**Tier I - $11.0M**	Northeast Illinois Regional Commuter Railroad Corporation	Commuter Rail
			Chicago Transit Authority	Heavy Rail
			Northern Indiana Commuter Transportation District	Commuter Rail
LA	New Orleans	Tier II	New Orleans Regional Transit Authority	Light Rail
MA	**Boston**	**Tier I - $9.6M**	Massachusetts Bay Transportation Authority	Commuter Rail, Heavy Rail, Light Rail
MI	Detroit	Tier II	City of Detroit Department of Transportation	Other Rail (AG)
MN	Twin Cities Area	Tier II	Metro Transit	Light Rail
MO	Saint Louis	Tier II	Bi-State Development Agency	Light Rail
NY	Buffalo	Tier II	Niagara Frontier Transp. Authority	Light Rail

[3] The DC SAA will administer these funds
[4] The IL SAA will administer these funds

State	Urban Area	Regional Allocation/Eligibility	Eligible System	Eligible Mode
NY/NJ/CT[5]	**New York City/Jersey City/Newark**	**Tier I - $47.0M**	Metropolitan Transportation Authority	Heavy Rail, Commuter Rail
			Port Authority of New York and New Jersey	Heavy Rail
			New Jersey Transit Corporation	Light Rail, Commuter Rail
			Connecticut Department of Transportation	Commuter Rail
OH	Cleveland	Tier II	The Greater Cleveland Regional Transit Authority	Heavy Rail, Light Rail
OR	Portland	Tier II	Tri-County Metropolitan Transportation District of Oregon	Light Rail
PA	Pittsburgh	Tier II	Cambria County Transit Authority	Other Rail (IP)
			Port Authority of Allegheny County	Light Rail, Other Rail (IP)
PA/NJ	**Philadelphia**	**Tier I - $8.0M**	Pennsylvania Department of Transportation	Commuter Rail
			Southeastern Pennsylvania Transportation Authority	Commuter Rail, Heavy Rail, Light Rail
			Port Authority Transit Corporation	Heavy Rail
			New Jersey Transit Corporation	Commuter Rail
TN	Memphis	Tier II	Memphis Area Transit Authority	Light Rail
TX	Dallas/Fort Worth/Arlington	Tier II	Dallas Area Rapid Transit	Light Rail
			Trinity Railway Express	Commuter Rail
	Houston	Tier II	Metropolitan Transit Authority Of Harris County	Light Rail
WA	Seattle	Tier II	Central Puget Sound Regional Transit Authority	Commuter Rail, Light Rail

[5] The NY SAA will administer these funds

FY 2006 TSGP Eligible Intracity Bus Systems

State	Urban Area	Regional Allocation/Eligibility	Eligible System[6]
AZ	Phoenix		*Valley Metro Regional Public Transportation Authority*
			City of Phoenix Public Transit Department
CA	**Bay Area**	Tier I - **$2.1M**	Alameda-Contra Costa Transit District
			Golden Gate Bridge, Highway and Transportation District
			San Francisco Bay Municipal Transportation Authority
			Santa Clara Valley Transportation Authority
			Central Contra Costa Transit Authority
			San Mateo County Transit District
			Caltrans (Transbay Bus Terminal)
	Greater Los Angeles Area (Los Angeles/Long Beach and Anaheim/Santa Ana UASI Areas)	Tier I - **$2.2M**	Los Angeles County Metro Transportation Authority
			Orange County Transportation Authority
			City of Los Angeles Department of Transportation
			Foothill Transit
			Santa Monica's Big Blue Bus
			Long Beach Transit
	San Diego	Tier II	San Diego Metropolitan Transit System
			North San Diego County Transit District
CO	Denver	Tier II	Denver Regional Transportation District
DC/MD/VA	**Greater National Capital Region (NCR and Baltimore UASI Areas)**	Tier I - **$1.3M**	Washington Metropolitan Area Transit Authority
			Maryland Transit Administration
			Ride-On Montgomery County Transit
			Prince George's County Transit
			City of Alexandria - Alexandria Transit Company
			Fairfax Connector Bus System
			Potomac and Rappahannock Transportation Commission
FL	Miami/Fort Lauderdale	Tier II	Miami-Dade Transit
			Broward County Mass Transit Division
GA	Atlanta	Tier II	Metropolitan Atlanta Rapid Transit Authority
			Georgia Regional Transportation Authority
HI	Honolulu	Tier II	City and County of Honolulu Department of Transportation Services
IL/IN	**Chicago**	Tier I - **$1.5M**	Chicago Transit Authority
			Pace - Suburban Bus Division
LA	New Orleans	Tier II	*New Orleans Regional Transit Authority*
			Jefferson Parish Department of Transit Administration
MA	**Boston**	Tier I - **$1.0M**	Massachusetts Bay Transportation Authority
MI	Detroit	Tier II	*City of Detroit Department of Transportation*
			Suburban Mobility Authority for Regional Transportation
MN	Twin Cities Area	Tier II	Metro Transit
MO	St. Louis	Tier II	*Bi-State Development Agency*
			Madison County Transit District
NV	Las Vegas	Tier II	Regional Transportation Commission of Southern Nevada

[6] Phoenix, Cincinnati, and San Antonio are newly eligible urban areas for this program in 2006; those systems identified in italics are newly eligible in 2006. Transit systems in Cleveland, Detroit, New Orleans, and St. Louis are newly eligible for bus grants.

State	Urban Area	Regional Allocation/Eligibility	Eligible System[7]
NY/NJ/CT	**New York City/ Jersey City/ Newark**	Tier I - **$5.5M**	Metropolitan Transportation Authority
			New Jersey Transit Corporation
			Westchester County Department of Transportation
			Port Authority of New York and New Jersey (PANYNJ Manhattan Bus Terminals)
OH	Cincinnati	Tier II	*Southwest Ohio Regional Transit Authority*
			Transit Authority of Northern Kentucky
	Cleveland	Tier II	*The Greater Cleveland Regional Transit Authority*
OR	Portland		Tri-County Metropolitan Transportation District of Oregon
			Clark County Public Transportation Benefit Area Authority
PA	Pittsburgh	Tier II	Port Authority of Allegheny County
PA/NJ	**Philadelphia**	Tier I - **$1.4M**	Southeastern Pennsylvania Transportation Authority
			New Jersey Transit Corporation
TX	Dallas/Forth Worth/Arlington	Tier II	Dallas Rapid Area Transit
			Ft. Worth Transportation Authority
	Houston	Tier II	Metropolitan Transit Auth. Of Harris County
			Island Transit
	San Antonio	Tier II	*VIA Metropolitan Transit*
WA	Seattle	Tier II	King County Department of Transportation - Metro Transit Division
			Pierce County Transportation Benefit Area Authority
			Snohomish County Transportation Benefit Area Corporation
WI	Milwaukee	Tier II	Milwaukee County Transit System

FY 2006 TSGP Eligible Ferry Systems

State	Urban Area	FY 2006 Regional Allocation	Eligible System[8]
CA	Bay Area	$700,000	Golden Gate Bridge, Highway and Transportation District
			City of Alameda Ferry Services (Blue and Gold Lines Fleet)
			City of Vallejo Transportation Program
LA	New Orleans	$300,000	Crescent City Connection Division - Louisiana Department of Transportation
MA	Boston	$400,000	Massachusetts Bay Transportation Authority
NY/NJ	New York City	$1,300,000	New York City Department of Transportation
			Port Authority of Trans Hudson Corporation
TX	Houston	$300,000	Texas DOT (Bolivar Roads Ferry)
WA	Seattle	$2,000,000	Washington State Ferries

[7] Phoenix, Cincinnati, and San Antonio are newly eligible urban areas for this program in 2006; those systems identified in italics are newly eligible in 2006. Transit systems in Cleveland, Detroit, New Orleans, and St. Louis are newly eligible for bus grants.

[8] Those systems identified in italics are newly eligible in 2006.

Program Coordination

The following entities were involved in developing the FY 2006 TSGP guidance:

- *Department of Homeland Security:* Office of Grants and Training; Transportation Security Administration; Office of Infrastructure Protection; Science and Technology Directorate; United States Coast Guard; Office of the Chief Intelligence Officer
- *Department of Transportation:* Federal Transit Administration
- *Industry:* American Public Transportation Association; various individual transit system owners and operators.

This grant program was also informed by ongoing discussions with State and local law enforcement officials regarding infrastructure protection priorities.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Transit Security Grant Program are available at the following web link: www.grants.gov.

FY 2006 Intercity Bus Security Grant Program (IBSGP)

Purpose

The purpose of the FY 2006 IBSGP is to create a sustainable program for the protection of intercity bus systems and the traveling public from terrorism, especially explosives and non-conventional threats that would cause major loss of life and severe disruption.

The FY 2006 IBSGP also seeks to assist owners and operators of fixed route intercity and charter bus services in obtaining the resources required to support the Goal and the associated National Priorities. Through its focus on enhanced planning, facility security enhancements, vehicle and driver protection, as well as training and exercises, the FY 2006 IBSGP directly addresses five of the seven National Priorities:

1. Implementing the National Incident Management System and the National Response Plan;
2. Implementing the National Infrastructure Protection Plan;
3. Strengthening information sharing and collaboration capabilities;
4. Enhancing interoperable communications capabilities; and,
5. Strengthening chemical, biological, radiological, nuclear and explosive detection and response capabilities.

In addition, the FY 2006 IBSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the intercity bus industry.

Funding

Provides **$9,503,000** to owners/operators of fixed route intercity and charter bus services using over-the-road buses.

Solicitation

The FY 2006 IBSGP is the fourth round of grants and builds upon the previous three rounds. *Successful applications will be selected through a competitive process.* The FY 2006 program focuses on the following national intercity bus security priorities:

- Facility security enhancements in defined Urban Area Security Initiative jurisdictions;
- Driver security enhancements;
- Vehicle security enhancements;
- Emergency communication technology;
- Coordinating with local police and emergency responders; and,
- Training and exercises.

Each of these priorities further enhances efforts for prevention and protection against terrorist activities and will greatly serve to assist with response and recovery efforts in the event of an attack.

Eligible applicants may submit one application for funding of up to three individual projects that address the priorities identified in this section. Funding may be awarded for all, some or none of the projects submitted based on the outcome of this evaluation process.

Project Selection

Each application will be evaluated by a National Review Panel. Federal staff from TSA and the U.S. Department of Transportation's Federal Motor Carrier Safety Administration (FMCSA) and G&T will evaluate proposals as part of the National Review Panel. The following method of selection will be followed under this program:

1. G&T will verify compliance with each of the administrative and eligibility criteria identified in the application kit;
2. Eligible applications will be reviewed and scored by a National Review Panel against the evaluation criteria;
3. The National Review Panel will create a rank order listing of proposed projects;
4. TSA and Preparedness Directorate staff will review the National Review Panel recommendations and make final selections for funding. As part of the final selection process, DHS staff will coordinate facility security enhancement projects identified for funding with the State Administrative Agencies (SAA) and Homeland Security Advisors (HSA) in the affected states to ensure consistency with the State and Urban Area Homeland Security strategies. Both the SAA's and HSA's inputs will be factored into the final decision making process; and,
5. TSA will brief all appropriate agencies on the final selections to ensure agreement for each grant work plan.

Eligibility

Funding under this program will be limited to owners/operators of fixed route intercity and/or charter bus services using over-the-road buses.

Fixed route, intercity bus service is defined as passenger transportation service provided to the general public for compensation over specified, pre-determined, and published routes between cities or terminals using over-the-road-buses. Eligible fixed route and charter services use over-the-road buses, provide trips annually to a defined Urban Area Security Initiative (UASI) jurisdiction or a facility located within a UASI jurisdiction. An over-the-road bus is defined as a vehicle designated for long-distance transportation of passengers, characterized by integral construction with an elevated passenger deck located over a baggage compartment and at least 35 feet in length with a capacity of more than 30 passengers.

Grantees must develop and implement a Security and Emergency Preparedness Plan (SEPP) within one year of the award. The SEPP is based on a model developed by the American Bus Association/United Motorcoach Association Joint Venture. Technical support for the development of the SEPP is available from the Joint Venture.

Program Coordination

The following entities were involved in developing the FY 2006 IBSGP guidance:

- *Department of Homeland Security:* Office of Grants and Training; Transportation Security Administration; Office of the Chief Intelligence Officer
- *Department of Transportation:* Federal Motor Carriers Safety Administration
- *Industry:* American Bus Association; United Motorcoach Association; various individual bus owners and operators

This grant program was also informed by ongoing discussions with State and local law enforcement officials regarding infrastructure protection priorities.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Intercity Bus Security Grant Program are available at the following web link: www.grants.gov.

FY 2006 Intercity Passenger Rail Security Grant Program (IPRSGP)

Purpose

The purpose of the FY 2006 IPRSGP is to maintain a sustainable program for the protection of our nation's intercity passenger trains and the traveling public from terrorism, especially explosives and non-conventional threats that would cause major loss of life and severe disruption. Financial assistance is provided solely to Amtrak.

The FY 2006 IPRSGP also seeks to assist Amtrak in obtaining the resources required to support the Goal and the associated National Priorities. Through its focus on regional planning, infrastructure protection, improvised explosive devices and other non-conventional methods of attack, as well as training and exercises, the FY 2006 IPRSGP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System and the National Response Plan;
3. Implementing the National Infrastructure Protection Plan;
4. Strengthening information sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and,
6. Strengthening chemical, biological, radiological, nuclear and explosive detection and response capabilities.

In addition, the FY 2006 IPRSGP also supports strengthening emergency operations planning and citizen protection capabilities and assists in addressing security priorities specific to intercity passenger rail service.

Funding

Provides **$7,242,855** in grant funding to Amtrak to continue security enhancements for intercity passenger rail operations in the Northeast Corridor (service between Washington, DC, and Boston), Amtrak's hub in Chicago and expand these enhancements into the West Coast Service Area in key, high-risk urban areas (Seattle, Sacramento, Oakland, San Jose, Los Angeles

Eligibility

The FY 2006 DHS Appropriations Act provided funds for a discretionary grant program to address security enhancements for intercity passenger rail transportation. As part of the FY 2006 IPRSGP, the Department will partner with Amtrak, the major national passenger railroad, to develop security enhancements for intercity passenger rail operations. ***Amtrak is the only entity eligible to apply for funding under the FY 2006 IPRSGP.***

Project Selection

The expenditure of FY 2006 funding must directly support a risk-based Security and Emergency Preparedness Plan and must be coordinated with the Regional Transit Security Strategies (RTSS) in the National Capitol Region, Philadelphia, New York, Boston, Chicago, Seattle, Sacramento, Oakland, San Jose, Los Angeles and San Diego. To facilitate this coordination, Amtrak must provide a representative to the Regional Transit Security Working Groups responsible for the RTSS in these areas. Amtrak must also provide written certification that each applicable State Administrative Agency concurs that the required coordination with the RTSS has occurred.

Up to **50 percent** of the funds available through the FY 2006 IPRSGP will be available at the time of award to assist Amtrak in meeting its most pressing security needs in the Northeast Corridor and Chicago (as identified through the previous G&T-facilitated risk assessment for these areas). Amtrak may also use these funds for high priority projects (as identified through previously conducted site-specific vulnerability assessments) in its West Coast Service Area prior to completion of a required risk assessment for this part of its system. However, in order to allocate these funds, Amtrak must provide written certification that it has coordinated these expenditures with the applicable regional planning efforts. The remaining 50 percent of these funds will be released upon submission of the risk assessment for the West Coast Service Area.

Program Coordination

The following entities were involved in developing the FY 2006 IPRSGP guidance:

- *Department of Homeland Security:* Office of Grants and Training; Transportation Security Administration; Office of Infrastructure Protection; Science and Technology Directorate; Office of the Chief Intelligence Officer
- *Department of Transportation*: Federal Transit Administration; Federal Railroad Administration
- *Industry*: Association of American Railroads; American Public Transportation Association; National Railroad Passenger Corporation (Amtrak)

This grant program was also informed by ongoing discussions with State and local law enforcement officials regarding infrastructure protection priorities.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Intercity Passenger Rail Security Grant Program are available at the following web link: www.grants.gov.

FY 2006 Trucking Security Program (TSP)

Purpose

The purpose of the FY 2006 Trucking Security Program is to continue the Highway Watch® Program as a sustainable national program to enhance security and overall preparedness on our nation's highways.

The FY 2006 TSP also seeks to assist all professionals and operating entities throughout the entire highway sector in obtaining the skills and abilities required to support the Goal and the associated National Priorities. Through its focus on awareness training, reporting of suspicious incidents and information analysis, the FY 2006 TSP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration;
2. Implementing the National Incident Management System and the National Response Plan;
3. Implementing the National Infrastructure Protection Plan;
4. Strengthening information sharing and collaboration capabilities;
5. Enhancing interoperable communications capabilities; and,
6. Strengthening chemical, biological, radiological, nuclear and explosive detection and response capabilities.

In addition, the FY 2006 TSP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the trucking industry.

The TSP was originally developed in the trucking industry with an emphasis on safety. It has undergone a dramatic expansion with the grant funds provided by DHS in the three years from FY 2003 to FY 2005, and its benefits and resources are now available to all professionals and operating entities throughout the highway sector, including private companies, public entities and governmental operations.

Funding

Provides **$4,801,500** for the Highway Watch® Program.

Eligibility

As in prior years, eligibility for funding under this program will be limited to the American Trucking Associations as the program manager of Highway Watch®.

Program Highlights

The Highway Watch® program provides resources and services, free of charge, to intercity commercial bus and motorcoach operators, and school bus owners and operators; governmental entities; the companies and entities that build and maintain the highways; highway cargo facility operators and brokers; support

operations such as visitors centers, truck and bus support, and maintenance operations; commercial driver training schools and facilities; operators of private truck fleets; and public safety personnel, including law enforcement agencies that respond to emergencies on the highways; and any and all additional entities or stakeholder segments identified by Highway Watch® or TSA.

Highway Watch® recruits and trains highway professional to identify and report security and safety situations on our Nation's roads. The program operates and maintains a Highway Watch® Call Center in London, Kentucky, and also operates and maintains a Highway Information Sharing and Analysis Center located at the Transportation Security Operations Center in Herndon, Virginia.

By continuing to expand the scope of the existing Highway Watch® Program to encompass additional motor carriers and drivers in every state, territory, and Federal district in the country, all segments of the commercial motor carrier and transportation community can contribute to the security of the Nation.

Program Coordination

In developing the FY 2006 TSP guidance, the following entities were involved:

- *Department Of Homeland Security:* Office of Grants and Training; Transportation Security Administration; Office of Chief Intelligence Officer
- *Department Of Transportation:* Federal Motor Carriers Safety Administration
- *Industry:* American Trucking Associations; Commercial Vehicle Safety Association; American Association of State Highway and Transportation Officials; Owner Operator Independent Drivers Association; National School Bus Association

This grant program was also informed by ongoing discussions with State and local law enforcement officials regarding infrastructure protection priorities.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Trucking Security Program are available at the following web link: www.grants.gov.

FY 2006 Buffer Zone Protection Program (BZPP)

Purpose

The BZPP is a targeted infrastructure protection program that provides funds to build security and risk-management capabilities at the State and local levels that will help prevent and protect critical infrastructure from acts of terror. Specifically, the program helps to implement Buffer Zone Plans (BZPs) by providing funds to State and local agencies for planning and equipment acquisition. BZPs implement preventive and protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks within the immediate vicinity of high-risk critical infrastructure assets. BZPs are developed through cooperation among DHS, State and local officials and help increase the preparedness capabilities of the local jurisdictions.

Funding

Total funding in FY 2006 is **$48,015,000** for grants to help secure high-risk ciritical infrastructure sites in collaboration with State and local partners. The table below shows the state-by state allocations of BZPP funding.

FY 2006 BZPP Funding Allocations

States / Territories	Total Funding
Alabama	$378,000
Alaska	$1,189,000
Arizona	$567,000
Arkansas	$378,000
California	$5,835,000
Colorado	$189,000
Connecticut	$189,000
Delaware	$189,000
District of Columbia	$567,000
Florida	$1,701,000
Georgia	$567,000
Hawaii	$189,000
Idaho	$189,000
Illinois	$2,079,000
Indiana	$567,000
Iowa	$189,000
Kansas	$378,000
Kentucky	$567,000
Louisiana	$2,268,000
Maine	$189,000
Maryland	$756,000
Massachusetts	$2,134,000

States / Territories	Total Funding
Michigan	$1,945,000
Minnesota	$567,000
Mississippi	$189,000
Missouri	$756,000
Montana	$189,000
Nebraska	$189,000
Nevada	$1,189,000
New Hampshire	$189,000
New Jersey	$1,512,000
New Mexico	$189,000
New York	$6,591,000
North Carolina	$378,000
North Dakota	$500,000
Ohio	$1,323,000
Oklahoma	$189,000
Oregon	$189,000
Pennsylvania	$1,756,000
Puerto Rico	$189,000
Rhode island	$189,000
South Carolina	$756,000
South Dakota	$500,000
Tennessee	$945,000
Texas	$2,268,000
Utah	$378,000
Vermont	$189,000
Virginia	$945,000
Virgin Islands	$189,000
Washington	$1,756,000
West Virginia	$189,000
Wisconsin	$189,000
Wyoming	$189,000
Total	**$47,965,000**

Eligibility

The Governor of each State has designated an SAA to apply for and administer the funds under BZPP. The SAA is the only agency eligible to apply for BZPP funds and is responsible for obligating BZPP funds to the appropriate local units of government or other designated recipients. The SAA must coordinate all BZPP activities with the respective State Homeland Security Advisor.

Project Selection

The FY 2006 BZPP site selection process is built upon the DHS risk methodology. Identifying the risks to the nation's critical infrastructure is an important component of the Department's overall risk reduction programs. The FY 2006 iteration of the methodology represents a significant step forward in the analysis of the risk of terrorism faced by our Nation's communities. Gains have been made in both the quality and specificity of information and analysis incorporated within the model, yielding the most accurate estimation possible of the *relative* risk of prospective grantees.

1. Critical Infrastructure/Key Resources (CI/KR) sites in the National Asset Database have been selected for participation in the FY 2006 BZPP using a risk-based analytic approach. The Department, working with its partners in each State and representatives of the 17 critical infrastructure sectors, has identified those sites in the United States that represent the most at risk critical infrastructures based on an analysis of consequence, and available vulnerability and threat data.
2. Asset-based risks were used to guide the allocation of funds to specific sites within the United States. This approach generates risk reduction benefits for the greater community as well as at each site.
3. State allocations were determined based on the number of higher-risk sites.

Site-Specific Analysis. DHS worked with SSAs, States, and the private sector to identify the top 100 sites for each sector and evaluated them to determine which could have significant effect if lost or disrupted, as well as those sites that could have a regional or cross-jurisdictional impact if lost or disrupted. DHS then conducted vulnerability and threat analysis to evaluate how likely an attacker would be to succeed in attacking these assets and how likely an attacker would be to attempt it. Based on the results of this analysis, DHS identified the list of the select high-risk sites for consideration in the FY 2006 BZPP by analyzing consequence, vulnerability, and threat.

Risk Analysis. In addition to site-specific risk analysis, an important component of the Buffer Zone process is its ancillary benefits to the surrounding community. Identification of high-risk jurisdictions helps ensure that the Buffer Zone Protection Program will reduce risk to a broader array of at-risk assets, as well as enhance the preparedness of State and local governments.

The Department's methodology to determine high-risk jurisdictions brings together two separate, but complementary, types of risk: ***asset-based risk*** and ***geographically-based risk***. Considered together, these two calculations provide an estimate of total terrorism risk to a given region, evaluating both risks to assets within a State or territory, as well as risk related to the unique characteristics of the candidate States, territories, and the District of Columbia.

Program Highlights

- Resources are allocated to jurisdictions responsible for the selected CI/KR sites through the State Administrative Agency. The identified FY 2006 BZPP sites and their locations are considered sensitive, and therefore DHS provides each State with information regarding the identity and location of the assets. Jurisdictions who oversee these identified locations must complete Buffer Zone Plans for each of these identified sites.
- In developing the BZP, the responsible local jurisdiction(s) review and assess ways in which they can work with relevant Federal, State, local, tribal, and private sector agencies to coordinate their prevention and protection activities.
- The development of the BZP fosters a cooperative environment in which all relevant organizations can carry out their specific prevention and protection responsibilities more efficiently and effectively, while coordinating and leveraging existing programs and resources.
- In developing and implementing the BZPs, security and preparedness officials at all levels are encouraged to seek opportunities to coordinate and leverage funding from multiple sources, including Federal, State, and local resources.
- DHS provides a range of services to BZPP grantees and sub-grantees. This includes BZPP workshops, which train local law enforcement and homeland security personnel on the BZPP process, and on-site technical assistance for officials needing additional technical support in developing and/or implementing BZPs.

Program Coordination

In developing the FY 2006 BZPP guidance, the following entities were involved:

- *Department Of Homeland Security:* Office of Grants and Training; Office of Infrastructure Protection; Office of Chief Intelligence Officer
- *State and local:* Various local law enforcement, fire, and emergency response officials; State law enforcement officials, homeland security advisors, and emergency management officers.
- *Industry:* High-risk facility owners and operators.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Buffer Zone Protection Program are available at the following web link: www.grants.gov.

FY 2006 Chemical Sector Buffer Zone Protection Program (CHEM-BZPP)

Purpose

The CHEM-BZPP is a targeted infrastructure protection program that provides funds to build security and risk-management capabilities at the State and local levels that will help protect critical infrastructure in the national chemical sector from acts of terror. Specifically, the program helps to implement Buffer Zone Plans by providing funds to State and local agencies for planning and equipment acquisition. BZPs implement preventive and protective measures that make it more difficult for terrorists to conduct surveillance or launch attacks within the immediate vicinity of high-risk critical infrastructure assets. BZPs are developed through cooperation among DHS, State and local officials and help increase the preparedness capabilities of the local jurisdictions responsible for the security of surrounding communities.

CHEM-BZPP funding is focused on enhancing the protection of those critical infrastructures that, if attacked, could cause weapons of mass destruction-like effects, e.g., chemical storage and manufacturing facilities, refineries, etc. In light of several major new national planning priorities, which address such issues as the aftermath of Hurricane Katrina, the allowable scope of CHEM-BZPP activities includes catastrophic events, provided that these activities also build capabilities that relate to terrorism.

Funding

CHEM-BZPP provides **$25,000,000** to secure critical sites in the nation's chemical sector identified in collaboration with state and local partners. Through a partnership between the Preparedness Directorate's Office of Grants and Training and the Office of Infrastructure Protection, this targeted funding is available to responsible State and local jurisdictions to enhance their ability to protect and secure specific sites within the sector.

FY 2006 CHEM-BZPP Funding Allocations

States	Total Funding
Michigan	$1,553,000
California	$6,597,100
Illinois	$3,128,500
Indiana	$552,100
Texas	$5,109,700
New York	$654,000
New Jersey	$5,508,400
Pennsylvania	$1,266,900
Delaware	$630,300
Total	**$25,000,000**

Eligibility

The Governor of each State has designated an SAA to apply for and administer the funds under CHEM-BZPP. The SAA is the only agency eligible to apply for CHEM-BZPP funds and is responsible for obligating CHEM-BZPP funds to the appropriate local units of government or other designated recipients. The SAA must coordinate all CHEM-BZPP activities with the respective State HSA.

Project Selection

The FY 2006 CHEM-BZPP selection process is built upon the DHS risk methodology. The FY 2006 iteration of the methodology represents a significant step forward in the analysis of the risk of terrorism faced by our Nation's communities. Gains have been made in both the quality and specificity of information and analysis incorporated within the model, yielding DHS' current best estimate of the *relative* risk of prospective grantees.

Site-Specific Analysis. The Department, working with its partners in each State and representatives of the 17 critical infrastructure sectors, has identified those sites in the United States that represent the most at risk critical infrastructures based on an analysis of consequence, and available vulnerability and threat data. Based on the results of this analysis, DHS identified the list of the select high-risk chemical sites for consideration in the FY 2006 CHEM-BZPP by analyzing consequence, vulnerability, and threat.

Community Preparedness. In addition to site-specific risk analysis, a primary component of the CHEM-BZPP process is its ancillary benefits to the surrounding community. This process helps ensure that the CHEM-BZPP will reduce risk to a broader array of at-risk chemical sector assets, as well as enhance the preparedness of State and local governments to deal with risks specific to the location of chemical infrastructure in their jurisdiction.

Defining the Regions. The chemical industry has tended to co-locate facilities in proximate geographical areas to reduce the costs and risks involved in transporting chemicals over long distances. This dense clustering of chemical facilities characterizes a Chemical Region, which is further defined by the identification of the primary focus sites (those DHS has determined have the highest risk potential) and the counties and or states in which they are located.

Assessing Off-Site Release Potential within Regions. Additionally, the number of chemical facilities having the potential for off-site impacts located in the Chemical Regions was determined, and weighted in direct proportion to the number of people potentially impacted. This created an off-site impact potential for each of the regions regardless of jurisdiction affected.

Assessing Overall Density of the Chemical Sector in the Regions. A third consideration was the overall number of chemical sector facilities in the region, without regard to off-site impact. This allowed the density of chemical

manufacturing in the region to be considered. The analysis of the potential for off-site impacts for the chemical sector facilities and the number of chemical plants in the counties augmented the Urban Area risk analysis to prioritize the Chemical Regions.

Promoting Collaborative Risk Management for Multi-State Risks. Potential off-site impacts are not constrained to the jurisdiction in which a chemical facility or cluster of facilities is located. While SAAs can assure that collaborative risk management takes place within their states, this distribution of funds also may require multi-state collaborative risk management. Those states where consequence management planning activities are interdependent in and around a chemical cluster will engage with the state and local authorities developing Chemical BZPs in neighboring jurisdictions to include multi-state planning.

Program Coordination

In developing the FY 2006 CHEM-BZPP guidance, the following entities were involved:

- *Department Of Homeland Security:* Office of Grants and Training; Office of Infrastructure Protection; Office of Chief Intelligence Officer
- *State and local:* Various local law enforcement, fire, and emergency response officials; State law enforcement officials, homeland security advisors, and emergency management officers.
- *Industry:* High-risk chemical facility owners and operators.

Program Guidelines and Application Kit

The complete program guidelines and application kit for the Chemical Sector Buffer Zone Protection Program are available at the following web link: www.grants.gov.

2005-2006 Legislation Related to Port Security

AB 280 (Oropeza) Applies the same misdemeanor weapons prohibitions and access limitations that currently exist for airport restricted areas to restricted areas of passenger vessel terminals in harbors and ports. Status: Chaptered by Secretary of State – Chapter 289, Statutes of 2005.

AB 1406 (Karnette): Requires the state Office of Homeland Security (OHS) to make determinations and recommendations relating to port security funding and report its findings to the Governor and Legislature. Status: Vetoed.

AB 2237 (Karnette): Requires that the annual report submitted to the Legislature by the Director of Homeland Security must also include a component pertaining to the protection of the state's harbor and port facilities and the commercial marine transportation sector from terrorist attack. Status: Senate Appropriations Committee.

AB 2274 (Karnette): Requires local, regional and state agencies responsible for emergency preparation and response activities to work with all harbor agencies to ensure integration of harbor agencies' respective emergency preparation, response and evacuation procedures with the agencies' activities. Status: Senate Appropriations Committee.

AB 2991 (Karnette): Authorizes a harbor agency to receive counterterrorism or antiterrorism funds to pay for port or harbor infrastructure. Status: Senate Appropriations Committee.

AJR 21 (Karnette) Calls upon the President and Congress to return a "fair share" of customs revenues to California in order to fund infrastructure and security improvements in California ports. Status: Chaptered by Secretary of State – Res. Chapter 21, Statutes of 2005.

SB 760 (Lowenthal): Imposes a $30 fee on each shipping container processed at the Ports of Los Angeles and Long Beach and specifies the allocation and expenditure of the container fee revenues for rail system improvements, port security and environmental pollution mitigation. Status: Held in Assembly Appropriations Committee at author's request.

SB 762 (Lowenthal): Allows harbor agencies to establish permit systems to authorize drivers and motor carriers to enter their ports. Status: Failed passage in Assembly Transportation Committee.

SB1266 (Perata): Transportation bond measure that includes $0.1 million for a Port Security Program that will provide grants to improve the security in and around the state's ports, including funding for equipment to better screen incoming and outgoing cargo. Status: Chaptered by Secretary of State – Chapter 25, Statutes of 2006.

SCA 29 (Morrow): Would amend the California Constitution to prohibit a state or local governmental entity that owns or operates a harbor or port facility from allowing an entity owned or controlled by a foreign government to manage or operate the harbor or port. Status: In Senate Transportation and Housing Committee.

SJR 26 (Morrow): Calls upon the President and Congress to exercise the utmost scrutiny in any decision affecting ports and maritime security in the United States. Status: In Senate Transportation and Housing Committee.

The Port of Humboldt Bay - Eureka, CA

Entity that owns / manages the port?

Humboldt is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port of Humboldt Bay is one of three operational divisions of the Humboldt Bay Harbor Recreation and Conservation District (the Harbor District).

The Harbor District is a Special District governed by five directly elected Commissioners with staggered four-year terms.

Is it considered an operating port?

No. Humboldt is not an operating port, but rather a landlord port – it leases port property to terminal operators who manage the loading and off-loading of vessels.

Type of goods moving through the port?

Forest products, paper pulp, raw timber.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 178,00 tons; Dry Bulk Cargo: 314,000 tons; Liquid Bulk Cargo: 261,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Containers: minimal.

Annual revenue / contribution to economy?

(Awaiting answer)

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

(Awaiting answer)

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security.
(Awaiting further answer)

Name and contact info for person in charge of port security at the port?

David Hull, Port Director
Humboldt Bay Harbor District
P.O. Box 1030
Eureka, CA 95502
Phone (707) 443-0801
Fax (707) 443-0800
E-mail: dhull@portofhumboldtbay.org

The Port of Stockton - Stockton, CA

Entity that owns / manages the port?

Stockton is not a Tidelands Trust port. The Port is a Special District governed by six Commissioners; three appointed by the Stockton City Council and three appointed by the San Joaquin County Board of Supervisors.

Is it considered an operating port?

Yes.

Type of goods moving through the port?

Rice, fertilizer, cement.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 239,000 tons; Dry Bulk Cargo: 1,849,000 tons; Liquid Bulk Cargo: 818,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Annual revenue / contribution to economy?

$31,676,000.

Creates 4,500 jobs (direct and indirect): $262 million total output of revenues, includes $14.6 million in state and local tax revenue and $28.4 million in federal tax revenue.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

$1.9 million.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Port Police Department.

Name and contact info for person in charge of port security at the port?

George Lerner, Chief, Port of Stockton Police Department
Port of Stockton
P.O. Box 2089
Stockton, CA 95201
Phone (209) 946-0246
Fax (209) 465-7244
E-mail: glerner@stocktonport.com

The Port of Sacramento – West Sacramento, CA

Entity that owns / manages the port?

Sacramento is not a Tidelands Trust port. The Port is a Special District governed by seven Commissioners: one appointed by Yolo County, one appointed by Sacramento County, one appointed by the City of Sacramento and four appointed by the City of West Sacramento.

Pending legislation, AB 2939 (Wolk), would change the governance to four appointees from the City of West Sacramento and one from Yolo County.

Is it considered an operating port?

Yes. Sacramento is currently transitioning from an operating to a landlord port.

Type of goods moving through the port?

Bagged rice, fertilizer, newsprint, aggregate, lumber, wheat, project cargo.

Amount of goods moved annually (tonnage/number of containers)?

Dry Bulk Cargo: 736,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Annual revenue / contribution to economy?

$6,000,000.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

$461,000.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Port Police Department.

Name and contact info for person in charge of port security at the port?

Janie Rankins-Mayle, Captain of Port Police
Port of Sacramento
1110 West Capitol Ave., 1st FL
West Sacramento,CA 95691-2717
Phone: (916) 373-5832
Fax: (916) 373-5834
E-mail: janier@cityofwestsacramento.org

The Port of Richmond - Richmond, CA

Entity that owns / manages the port?

Richmond is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city; the city council serves as the Port Commission.

Is it considered an operating port?

No. Richmond is not an operating port, but rather a landlord port – it leases port property to terminal operators who manage the loading and off-loading of vessels.

Type of goods moving through the port?

Petroleum, liquid bulk, automobiles and other bulk cargo.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 73,000 tons; Liquid Bulk Cargo: 83,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Containers: minimal.

Annual revenue / contribution to economy?

Approximately $5,000,000.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

$2,500,000.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security.

Name and contact info for person in charge of port security at the port?

Jim Matzorkis, Executive Director
Port of Richmond
P.O. Box 4046
Richmond, CA 94084
Phone (510) 215-4600
Fax (510) 233-3105
E-mail: richmondport@yahoo.com

The Port of San Francisco – San Francisco, CA

Entity that owns / manages the port?

San Francisco is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city and is governed by five Commissioners nominated by the Mayor and confirmed by the City Council.

Is it considered an operating port?

No. San Francisco is not an operating port, but rather a landlord port – it leases port property to terminal operators who manage the loading and off-loading of vessels.

Type of goods moving through the port?

Steel, aggregate, lumber, newsprint. Large ferry and excursion business: approximately 6 million passengers annually.

Large cruise business: approximately 250,000 passengers annually.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 586,000 tons; Dry Bulk: 1,600,000 tons; Liquid Bulk Cargo: 28,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Containers: minimal.

Annual revenue / contribution to economy?

$60,000,000.

Creates 30,000 jobs (direct and indirect). Generates $1.7 billion in general port activity.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

Approximately $5,000,000.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Contract with San Francisco Police Department. Some contract private security.

Name and contact info for person in charge of port security at the port?

Sidonie Sansom, Director of Homeland Security
Port of San Francisco
Pier One
San Francisco, CA 94111
Phone (415) 274-0400
Fax (415) 732-0400
E-mail: sidonie.sansom@sfport.com

The Port of Redwood City – Redwood City, CA

Entity that owns / manages the port?

Redwood City is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city and is governed by five Commissioners appointed by the City Council.

Is it considered an operating port?

Yes. Although the port is largely a landlord port, it does manage some operations.

Type of goods moving through the port?

Bulk, neo-bulk, and liquid cargoes.

Amount of goods moved annually (tonnage/number of containers)?

Dry Bulk Cargo: 1,908,000 tons.

Is it a container port or something else?

Principally handles bulk cargo.

Annual revenue / contribution to economy?

Approximately $6,000,000.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

$75,000.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Some contract private security.

Name and contact info for person in charge of port security at the port?

Eric Napralla, Assistant Manager of Operations
Port of Redwood City
675 Seaport Blvd.
Redwood City, CA 94063
Phone (650) 306-4150
Fax (650) 369-7636
E-mail: enapralla@redwoodcityport.com

The Port of Hueneme – Port Hueneme, CA

Entity that owns / manages the port?

Hueneme is not a Tidelands Trust port.

The Oxnard Harbor District is a Special District governed by five directly elected Commissioners with staggered four-year terms.

Is it considered an operating port?

Yes. Although the port is largely a landlord port, it does manage some operations.

Type of goods moving through the port?

Automobiles, fresh fruit and produce, forest products.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 1,182,000 tons; Dry Bulk Cargo: 3,200 tons; Liquid Bulk: 148,000 tons.

Containers: 25,500 TEUs annually.

Is it a container port or something else?

Principally handles bulk cargo. Handles some containers.

Annual revenue / contribution to economy?

$11,900,000.

Creates 3,800 jobs (direct and indirect). Generates $535 million in economic activity.

Has it received a federal designation as a strategic port?

Yes.

How much has the port received in federal DHS grant money in the last few years?

$890,000.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Some contract private security.

Name and contact info for person in charge of port security at the port?

Andru Ortiz, Director of Operations and Maintenance
Port of Hueneme
P.O. Box 608
Port Hueneme, CA 93044
Phone (805) 488-3677
Fax (805) 488-2620
E-mail: aortiz@portofhueneme.org

The Port of Long Beach – Long Beach, CA

Entity that owns / manages the port?

Long Beach is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city and is governed by five Commissioners nominated by the Mayor and confirmed by the City Council.

Is it considered an operating port?

No.

Type of goods moving through the port?

Machinery, vehicles, toys and sports equipment, bedding, plastic, organic chemicals.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 97,905,000 tons; Dry Bulk Cargo: 6,686,000 tons; Liquid Bulk: 32,541,000 tons.

Containers: 6.71 million TEUs annually.

Is it a container port or something else?

Container port.

Also handles bulk cargo.

Annual revenue / contribution to economy?

$140 million.

Creates 316,000 jobs in California (direct and indirect) and 1.4 million jobs nationally. Generates $5.4 billion in customs revenue; $47 billion in direct and indirect business sales; $14.5 billion in trade-related wages; and $4.9 billion in local, state and general tax revenue.

Has it received a federal designation as a strategic port?

Yes.

How much has the port received in federal DHS grant money in the last few years?

(Awaiting answer)

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Long Beach Police Department. Some contract private security.

Name and contact info for person in charge of port security at the port?

Cosmo Perrone, Director of Security
Port of Long Beach
P.O. Box 570
Long Beach, CA 90801
Phone (562) 590-4178
Fax (562) 901-1734
E-mail: perrone@polb.com

The Port of Oakland – Oakland, CA

Entity that owns / manages the port?

Oakland is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city and is governed by seven Commissioners nominated by the Mayor and confirmed by the City Council.

Is it considered an operating port?

No.

Type of goods moving through the port?

Beverages, machinery, wood pulp, iron, steel, edible fruit and nuts.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 25,584,000 tons; Liquid Bulk: 596,000 tons.

Containers: 2.27 million TEUs annually.

Is it a container port or something else?

Container port.

Also handles bulk cargo.

Annual revenue / contribution to economy?

$289.8 million (including airport, seaport and commercial real estate). Maritime: approximately $130 million.

Creates nearly 450,000 jobs (direct and indirect). Generates $56.3 billion in economic activity, including $12.3 billion in personal income and consumption expenditures, and $1.3 billion in state and local tax revenue.

Has it received a federal designation as a strategic port?

Yes.

How much has the port received in federal DHS grant money in the last few years?

$11.2 million.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Oakland Police Department. Some contract private security.

Name and contact info for person in charge of port security at the port?

Michael O'Brien, Port Facilities Security Officer
Port of Oakland
P.O. Box 2064
Oakland, CA 94604
Phone (510) 227-1303
Fax (510) 835-1641
E-mail: mobrien@portoakland.com

The Port of Los Angeles – San Pedro, CA

Entity that owns / manages the port?

Los Angeles is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a department of the city and is governed by five Commissioners nominated by the Mayor and confirmed by the City Council. The Commissioners serve at the pleasure of the Mayor.

Is it considered an operating port?

No.

Type of goods moving through the port?

Furniture, apparel, toys and sporting goods, vehicles and vehicle parts, and electronic products.

Large cruise business: approximately 1.2 million passengers annually.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 114,997,000 tons; Dry Bulk: 4,314,000 tons; Liquid Bulk: 12,798,000 tons.

Containers: 7.5 million TEUs annually.

Is it a container port or something else?

Container port.

Also handles bulk cargo.

Annual revenue / contribution to economy?

$368.8 million.

Creates 259,000 jobs (direct and indirect) in California, and 1.35 million jobs nationally. Generates $26.8 billion annually in industry sales; $8.4 billion annually in regional wages and salaries; $1.4 billion in state and local tax revenue.

Los Angeles is the busiest port in the United States, and the eighth busiest in the world.

Has it received a federal designation as a strategic port?

No.

How much has the port received in federal DHS grant money in the last few years?

$26.6 million.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Port Police Department.

Name and contact info for person in charge of port security at the port?

George Cummings, Director of Homeland Security
Port of Los Angeles
P.O. Box 151
San Pedro, CA 90733
Phone (310) 732-7678
Fax (310)
E-mail: gcummings@portla.org

The Port of San Diego – San Diego, CA

Entity that owns / manages the port?

San Diego is a Tidelands Trust port and manages port property through agreement with the State Lands Commission.

The Port is a Special District governed by seven Commissioners, all nominated by the respective Mayor and confirmed by the respective City Council: three from San Diego, and one each from Chula Vista, Coronado, National City, and Imperial City.

Is it considered an operating port?

Although the port is largely a landlord port, it does manage some operations.

Type of goods moving through the port?

Automobiles, lumber, produce, cement, sand and steel.

Amount of goods moved annually (tonnage/number of containers)?

General Cargo: 1,498,000 tons; Dry Bulk Cargo: 1,137,000 tons; Liquid Bulk: 127,000 tons.

Containers: 100,000 TEUs annually.

Is it a container port or something else?

Principally handles bulk cargo. Handles some containers.

Annual revenue / contribution to economy?

$112.9 million (including maritime and real estate). Maritime: $23.6 million.

Creates 59,000 jobs (direct and indirect). Generates $8.4 billion in economic activity.

Has it received a federal designation as a strategic port?

Yes.

How much has the port received in federal DHS grant money in the last few years?

$13.5 million.

What type of security personnel is utilized?

As with all ports, terminal operators are required by the Coast Guard to develop security plans and to manage those plans with the Coast Guard.

Port staff serves as Director of Security. Harbor Police. Some contract private security.

Name and contact info for person in charge of port security at the port?

Kirk Sanfilippo, Chief
San Diego Harbor Police Department
3380 N. Harbor Drive
San Diego, CA 92101
Phone (619) 686-6570
Fax (619) 686-6357
E-mail: ksanfili@portofsandiego.org

U.S. has big gaps in cargo container security, Senate study finds

By Toby Eckert
COPLEY NEWS SERVICE

March 30, 2006

WASHINGTON – The number of high-risk cargo containers inspected before entering the United States is "staggeringly low," and government efforts to keep terrorists from exploiting the system are riddled with blind spots, congressional investigators say in a report that will be released today.

The study, by a Senate Homeland Security subcommittee, is the latest to raise questions about whether the Bush administration and Congress have done enough to improve security at seaports, border crossings and other transportation hubs since the Sept. 11, 2001, terrorist attacks. Experts say the system is vulnerable to the smuggling of a nuclear, chemical or biological weapon, or a direct attack by terrorists intent on crippling the U.S. economy.

If an attack shut down the Los Angeles-Long Beach port complex, it would take $150 million a day out of the economy, the Congressional Budget Office concluded in a separate report.

Most of the concern is focused on the millions of boxcar-size cargo containers that flow into U.S. seaports and across land borders each year. Despite efforts to inspect more of the containers before they reach the United States, only a minuscule number are examined abroad; the system used to identify potentially troublesome cargo is unreliable; and a program that allows shippers to avoid some inspections is not closely monitored, the three-year subcommittee investigation concluded.

"If we think that the terrorists are going to ignore our vulnerabilities and not find the kinks in our supply chain, we are mistaken," said Sen. Norm Coleman, R-Minn., the panel's chairman.

Earlier this week, the subcommittee revealed that undercover investigators had brought enough radioactive material across the Mexican and Canadian borders to make two radiation-spewing "dirty bombs." It also criticized the slow pace of installing radiation detectors at U.S. seaports and initiatives to thwart the smuggling of nuclear materials abroad.

"We do not yet have a maximum effort on what everyone agrees is the biggest threat to the American public," former New Jersey Gov. Thomas Keane, who headed the federal commission that investigated the Sept. 11 attacks, told the subcommittee Tuesday.

Coleman and other lawmakers want the Department of Homeland Security to embrace technology being used at the port of Hong Kong that scans every container passing through two gates there. While the Bush administration has been skeptical of the program, which involves technology developed by San Diego-based SAIC, Homeland Security Secretary Michael Chertoff is traveling to Hong Kong this weekend for a demonstration.

The study that will be released today took a firsthand look at operations at 18 ports and border crossings in the United States and abroad, including the San Ysidro entry point and the Port of Los Angeles. It follows up on a similar report by the subcommittee last year.

While the investigators noted some improvements, they called their overall findings "troubling."

A central goal of the Homeland Security Department's strategy is to intercept dangerous cargo before it reaches U.S. shores, but the probe found major flaws in the effort. The Container Security Initiative, which has placed U.S. personnel at 44 international ports, is inspecting a "disturbingly low" number of containers identified as high-risk, the study said.

Slightly more than 37 percent of high-risk shipments were examined abroad, the investigators found. They attributed the low rate to "mission fatigue," given the large number of containers; lack of time and resources; and uncooperative foreign-port operators.

WSC / KOCH OUTLINES PROBLEMS WITH CARGO SCREENING LEGISLATION

World Shipping Council President Chris Koch submitted a letter to the House Homeland Security Committee, outlining the ocean carrier group's concerns with a proposed bill that would require all containers headed to the United States to first be scanned in foreign ports.

The "Sail Only if Scanned Act," or SOS bill, is expected to be offered as an amendment to a comprehensive piece of cargo and port security legislation, "The SAFE Port Act," that the committee is scheduled to edit and vote on next week after it returns from Easter recess.

The SOS bill, which originally was blocked by a subcommittee from being attached to the SAFE Port Act, "would cripple American commerce and almost certainly cause significant conflict with foreign governments," Koch said.

The legislation insists on 100 percent scanning of all containers within a year of passage.

Koch said the short-time frame, vague instructions and mandatory sanction to terminate trade with foreign ports that fail to conduct out-bound scans made implementation of the requirement unrealistic. Koch said the bill does not make clear what "scanned" means, as well as who is to do the scanning and how the system would work.

CBP is now able to check about half of all containers entering the country for radiation using large-scale detection machines and plans to have complete coverage by the end of 2007. The agency also takes X-ray or gamma ray images of about 5.5 percent of cargo containers from suspicious or unknown origins. Most of those non-intrusive exams are conducted on U.S. soil, but some are done by cooperating customs authorities in 43 foreign ports under the Container Security Initiative.

A new system developed and tested by the private sector in the Port of Hong Kong would combine radiation and imaging systems that could capture container data as trucks move through the terminal gate.

The proposed legislation does not indicate whether scanning should include radiation detection only, X-ray imaging, or both. The bill also does not spell out whether the data must be immediately analyzed or is simply captured for later use, and whether the security measures are to be conducted by the private sector or foreign governments.

Congress needs to clarify its vision for such an inspection regime because allowing foreign terminal operators to control data used for U.S. security purposes is inconsistent with the position it took during the Dubai Ports World case, when it forced the state-owned company in Dubai to divest its recently acquired operating rights in U.S. ports because of concerns that the company could not be trusted to load and unload vessels, Koch said.

Koch has urged Congress to let DHS continue studying the feasibility of employing the integrated scanning system being tested in Hong Kong, and to support CSI and other efforts to engage the cooperation of foreign governments and the private sector to verify the integrity of cargo at the foreign load point.

[American Shipper – 4.20.06]

WWW.SEAPORTSPR.COM
SEAPORTS Press Review
Tuesday, June 27, 2006 Vol

Port Services & Technology News

Cargo Container Security: Someone Must Take the Bull by the Horns

Thursday, June 22, 2006

(Oyster Bay, NY) - Governments and port authorities acknowledge that the 17 million cargo containers in use around the world are a weak link in national security arrangements. Import/exporters and manufacturers understand that poor container security poses a risk to the goods they contain. Yet because there are so many players in the global freight ecosystem, and the problem is distributed in thousands of ports and transport hubs around the world, attempts to improve it have been inadequate.

"Efforts underway in the ISO to create a uniform standard for electronic container security should bear fruit within the next 12 months," says ABI Research analyst Robert Foppiani. "But getting shippers and port operators to comply and to invest in costly systems that provide little or no ROI is another matter. Everyone wants to improve security, but all the maritime industry players are looking to each other to be the first to invest. An organization such as the World Customs Organization needs to mandate electronic seal standards. Until some of these stakeholders make hard decisions, the situation will remain unsatisfactory."

Several manufacturers—General Electric, Savi Technology and IBM—are designing electronic container security systems. GE's is called "CommerceGuard." ABI Research has examined its key elements and found shortcomings that highlight some of the critical issues facing any attempt to secure containers.

CommerceGuard is a proprietary system. That seems a major drawback for a system which, to be effective, must work identically in thousands of facilities worldwide.

In addition, unlike other systems that use disposable tags, CommerceGuard's are reusable, implying a massive "recycling" operation to move used tags to their next point of use. Shippers are unlikely to accept any such solution.

"Because the container electronic security market is still quite immature, it is difficult for government to specify a single technology as a cure-all solution," concludes Foppiani. "But until something is done, security will continue to suffer."

ABI Research's new study, Cargo Container Security Tracking, examines and evaluates evolving solutions and technologies for global electronic container security tracking. It forms part of the RFID and Commercial Telematics Research Services.

Founded in 1990 and headquartered in New York, ABI Research maintains global operations supporting annual research programs, intelligence services and market reports in broadband and multimedia, RFID and M2M, wireless connectivity, mobile wireless, transportation and emerging technologies. For information visit www.abiresearch.com, or call +1.516.624.2500.

Contact:
Beth Schechner | Tel: 516-624-2542 |
Fax: 516-624-3115 | pr@abiresearch.com

Commonwealth
BUSINESS • MEDIA

SEAPORTS PUBLICATIONS GROUP
Commonwealth Business Media, Inc.
Ray Venturino, Publisher
33 Washington Street, 13th Floor
Newark, NJ 07102-3107 Tel: (973) 848-7207

Email: **rventurino@joc.com**

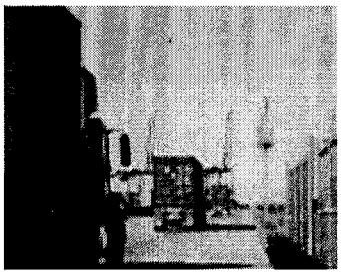
Seaports PUBLICATIONS

TERMINALS, UNIONS: TWIC NEEDS TWEAK

The federal government plans to issue the first TWIC cards by the end of the year, but marine terminal operators and labor unions say the program could cause delays at seaports and will hold Americans to a higher standard than foreign-born workers.

Industry representatives are urging the government to refine the process of background checks before issuing identification cards to as many as 750,000 longshoremen, merchant mariners, harbor truck drivers and other transportation workers at the nation's ports.

The card is a biometric identification credential that transportation industry workers who require unescorted access to facilities such as marine terminals will eventually have to use.



For example, a harbor truck driver will need a TWIC card to enter a marine terminal gate and spot the container inside the terminal.

Security officers at marine terminals in Los Angeles-Long Beach warned that proposed government standards for use of the TWIC card could lengthen from a few seconds to a few minutes the time it takes for a longshoreman or truck driver to gain access to the facility. For a typical Southern California marine terminal that handles 1 million TEUs per year and processes 3,000 truck moves a day, the snowballing impact of the delays could severely disrupt the flow of cargo, terminal operators say.

Terminal executives also expressed concern about use of the contact chips embedded in prototype TWIC cards the government has been testing. They predicted that the proposed cards and electronic readers could experience hardware problems in the harsh marine terminal environment.

Representatives of the International Longshore and Warehouse Union and seafaring unions also criticized the background checks that workers will undergo to qualify for TWIC cards. The government has almost unlimited ability to check into the criminal history of the U.S.-born longshoremen and merchant mariners that comprise the vast majority of the unions' membership.

For example, the government has easy access to background information on American workers who years ago may have been convicted of offenses that could result at least in interim disqualification from receiving a TWIC card. Such disqualifying offenses include sexual abuse, robbery or distribution of narcotics, crimes that have nothing to do with homeland security, the unions stated.

But the U.S. government has little if any access to background information on the foreign-born merchant mariners that work on 95 percent of the vessels that call at U.S. ports, or to the many immigrant truck drivers who work at the ports. Union spokesmen noted that in most cases the foreign governments would refuse to supply such information to the U.S. even if the

background information from other countries could indicate the foreign-born workers have terrorist ties.

[Source: JOURNAL of COMMERCE ONLINE www.joc.com 6.07.06]

CQ HOMELAND SECURITY - INDUSTRY & CONTRACTING
April 24, 2006 - 7:38 p.m.

Law May Require TSA to Use Airport Group's Background Check System for TWIC

By Angela Kim, CQ Staff

The Transportation Security Administration may be required by law to use an airport lobby group's background check system to implement the agency's long-awaited credentialing program for maritime port workers, possibly doing away with some or all competitive contracting.

TSA has been trying in fits and starts to implement its Transportation Worker Identification Credential (TWIC) program for the past three years.

The agency in the past month issued two solicitation notices to find a contractor to run the program. The first stated that the agency was looking to award a single-source contract to manage the whole program.

That notice was revised last week to say the agency wants a vendor or possibly multiple vendors to enroll workers in TWIC and manage the help desk and call center. The identity management system (IDMS) portion - arguably the most significant part of the contract involving collection of biometric data and card issuance and revocation - was excluded from the second solicitation notice.

According to a provision in Section 528 of the fiscal year 2006 homeland security appropriations bill (PL-109-90), TSA parent Department of Homeland Security could be required to use a group called the Transportation Security Clearinghouse "as the central identity management system for the deployment and operation" of credentialing programs, including TWIC and Registered Traveler.

Run by the airport lobbying group American Association of Airport Executives (AAAE), the Transportation Security Clearinghouse has conducted background checks for other federal security programs involving workers in the commercial and general aviation industries.

The clearinghouse charges a fee to collect fingerprints and personal information from airline and airport workers and send the data over a secure connection to the federal government for criminal history checks against FBI databases. The clearinghouse also conducts background checks for foreign-born flight students seeking training in the United States.

The clearinghouse traditionally has left issuance of biometrically enabled access cards to the airports or airlines that work with other contractors to issue the cards once workers are approved through the background check process.

TWIC requires the federal government to issue a universal biometrically enabled ID.

AAAE Senior Vice President for Transportation Security Policy Carter Morris said the clearinghouse has been in talks with TSA to offer its services to create a public-private partnership that would manage TWIC.

The language in the homeland security appropriations law "could be interpreted as a mandate," Morris said, speaking by phone from the association's annual conference in San Diego. But the clearinghouse is not necessarily pushing that interpretation.

"It's not my job to interpret the law," Morris said, but the clearinghouse wants TSA to know that it can help with TWIC implementation if the agency chooses.

"If it makes sense, great, if it doesn't, no one is going to blame [TSA]," he said.

Morris added that the clearinghouse has a proven track record, having processed more than 2 million employee checks to date. The group checks out on average 2,000 aviation workers a day and "we haven't even touched our bandwidth or capacity," he said. Although the clearinghouse has focused on the aviation industry, Morris believes that it also would be able to meet "the unique needs and customer service requirements" of the maritime port industry.

The airport group's services could be cost-effective both "in terms of time in implementation" as well as the fee that would be necessary to pay for the program because TWIC would "build off what already exists," Morris said.

The clearinghouse could meet DHS' end-of-year deadline to finally roll out TWIC, according to Morris.

For its part, TSA Monday said it is staying on course with its current contracting strategy to find a vendor that can carry out enrollment and provide technical support.

TSA "is focusing [its] contracting resources on [the enrollment and help desk] portion," an agency spokesman said. "We are considering and evaluating our options for the IDMS portion of the contract."

A mandate to use the clearinghouse for a part or all of the TWIC contract could leave potential contractors such as Lockheed Martin and TWIC prototype vendor BearingPoint in the cold.

New York-based Verified Identity Pass, which has a partnership with Lockheed to bid for the TWIC contract, declined to comment further about the program implementation yesterday.

The Homeland Security Appropriations Committee was not available for comment as of press time.

Section 528 of the homeland security appropriations bill in question says: "The Secretary of Homeland Security shall utilize the Transportation Security Clearinghouse as the central identity management system for the deployment and operation of the registered traveler program and the transportation worker identification credential program for the purposes of collecting and aggregating biometric data necessary for background vetting; providing all associated record-keeping, customer service, and related functions; ensuring interoperability between different airports and vendors; and acting as a central activation, revocation, and transaction hub for participating airports, ports, and other points of presence."

Expert warns of port terror dwarfing Sept. 11 toll

Local conference features dire warnings about port security, cost of attack.

By Troy Anderson, Staff writer
Long Beach Press Telegram

It's been nearly five years since terrorists attacked the United States, but local experts predicted Wednesday that there will be another attack that will make Sept. 11, 2001, "look like peanuts."

And a likely scenario involves separate or simultaneous attacks on the nation's largest ports Los Angeles/Long Beach, New York City/New Jersey and Houston that could cripple the nation's economy.

"Instead of talking 3,000 casualties, we are going to be talking about hundreds of thousands, or millions of casualties," said Mike Intriligator, one of the nation's leading economists and a professor of economics, political science and public policy at UCLA.

Intriligator said the federal government has not responded innovatively to protect the country and instead has created a bureaucracy with the U.S. Department of Homeland Security.

"I think we're going to pay a big price for that because in my view I think we're still extremely vulnerable," Intriligator said. "I think we are facing a huge threat."

Intriligator was one of more than a dozen speakers at a conference on terrorism Wednesday hosted by the U.S. Department of Homeland Security-funded Center for Risk and Economic Analysis of Terrorism Events, based out of USC.

Jim Moore II, a professor of industrial and systems engineering at the university, said research on the impact of a "dirty bomb" or other weapon of mass destruction at the nation's three largest port complexes found it would cost the economy tens of billions of dollars a month.

A large attack on the ports in Los Angeles and Long Beach alone would have a $23 billion-a-month impact on the local economy.

In his study, Moore wrote it is well known that ports have been vulnerable since 2001 because of the infrequency of container checks. He noted that officials have replaced handheld radiation detectors with stationary radiation screening devices to screen containers coming through the ports since new rules went into effect in 2004.

"However, these more advanced measures will not be in place until much later, and their effectiveness has yet to be tested," Moore wrote.

But Rachel Campbell, a spokeswoman for the Port of Los Angeles, defended port security efforts and said the economic impact of an attack would be mitigated by transferring cargo shipments to other ports around the nation.

"Also, we have put in place a myriad of new security enhancements at the port. And we have the U.S. Coast Guard, U.S. Customs, FBI and all of the local law enforcement agencies, including the LAPD, CHP, Long Beach police and our own L.A. Port Police.

"We're one of the few ports in the nation to have our own police force exclusively dedicated to us."

Still, conference keynote speaker Rear Admiral William D. Sullivan, vice director for strategic plans and policy for the United States Department of Defense, said al-Qaida's goal is to bankrupt the nation and force it to withdraw its troops from the Middle East.

"There is no question if you look at what we've spent in the last 4 years on homeland security and terrorism that it's staggering," Sullivan said.

Gary Becker, a senior economist at the Department of Homeland Security, said the Congressional Budget Office has estimated the annual cost of fighting terrorism at tens of billions of dollars.

But he said that doesn't take into account many variables, such as delays at airports and the borders and other factors.

"We really don't know a whole lot about the overall costs and benefits of homeland security," Becker said.

At the conference, speakers recommended that experts further study the costs and benefits of homeland security and refine the new risk-based method of allocating the money to ensure that cities and states with the most likely targets get their fair share of the funding.

Intriligator recommended that the Central Intelligence Agency and National Security Agency begin working together and sharing intelligence and he suggested that jurisdictions nationwide should emulate the county's Terrorism Early Warning Group, which holds regular intelligence briefings.

"I think it's a model for the world," Intriligator said. "Al-Qaida's goal is to kill 4 million Americans. The big one is coming, but it's not an earthquake. It's a terrorist strike."

1372-S

Additional copies of this publication may be purchased for $10 per copy (includes shipping and handling), **plus current California sales tax**.

Senate Publications & Flags

1020 N Street, B-53

Sacramento, CA 95814

(916) 651-1538

Make checks or money orders payable to **Senate Rules Committee**. Credit cards not accepted.

Please include Stock Number **1372-S** when ordering.