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.