

STATEMENT OF
MATTHEW R. BETTENHAUSEN
DIRECTOR,
CALIFORNIA OFFICE OF HOMELAND SECURITY
BEFORE THE
LITTLE HOOVER COMMISSION
JANUARY 26, 2006

Mr. Chairman and members of the Commission: Thank you for the opportunity to testify before you again. My name is Matthew Bettenhausen and I am the Director of the California Office of Homeland Security.

I am pleased to be here with my partner, a seasoned emergency manager and leader, Mr. Henry Renteria, the Director of the Governor's Office of Emergency Services. He has made my time in California both professionally rewarding and purposeful. I appreciate the commitment he brings to emergency preparedness and the spirit of teamwork he has fostered throughout his department.

As evidence of this teamwork, and since the Commission asked us both to address the same questions in our testimony today, we have divided the labor, or the opportunity if you will, of responding to your inquires. I will address our efforts to prevent and prepare for catastrophic events that could overwhelm local jurisdictions. Specifically, I will focus on the threats facing California, how preparedness planning has evolved to better counter these threats, and how we have invested resources to minimize the risks and consequences associated with these risks.

CALIFORNIA IS A HIGH RISK STATE

California continues to be a high risk state with a wide variety of potential targets. With its large urban areas and enormously diverse cultural landscape, California offers terrorists ideal opportunities for concealment, as well as possible recruitment and logistical support.

California is home to the world's sixth largest economy. We are home to 12% of the nation's population. And, as the Governor said, we are home to the California dream.

To protect these assets, we must remain vigilant. And we can not allow the absence of a successful terrorist attack to lull us into a false sense of security. Indeed, the footprints of terrorists and their organizations have been discovered throughout California.

For example, earlier this summer, authorities thwarted a terrorist attack orchestrated from the depths of Folsom Prison when inmates there were tied to a terror case. Two Folsom state prison inmates and a parolee are at the center of a federal investigation into an alleged terrorist plot with potential targets in Southern California that included National Guard facilities, synagogues and the Israeli consulate in Los Angeles.

Investigations are focusing on an Islamic extremist group JIS (Jamiyyat Ul Islam Is Saheeh) that operates at Folsom prison. The radicalization of inmates is very real and poses a major problem and challenge.

In another investigation, it was discovered that a Lodi man, Hamid Hayat, participated in an al Qaeda sponsored terrorist training camp. Mr. Hayat's goal was allegedly to commit jihad in the United States.

In another case, on May 27, 2005, the U.S. Immigration and Customs Enforcement (ICE) deported to Pakistan an individual (Khamal Muhammad, 23) who resided in the San Francisco Bay Area and was an admitted member of a U.S.-designated terrorist organization in Pakistan - the Harakat ul Mujahidin (HUM) organization. Mr. Muhammad admitted to attending a HUM training camp where he received training in the use of pistols, rifles and grenades.

More significantly, Al Qaeda had its sights set on California as part of “planes operation” that resulted in the 9/11 attacks. Ramzi Yousef was advancing a plan called “Project Bojinka”, Serbo Croatian for “Big Bang”, which envisioned a second wave of airplane attacks targeting sites on the West Coast.

As part of the terrorist attacks of 9/11, we know that two of the terrorists lived and conspired in the San Diego area prior to participating in these cruel attacks on Washington, New York and Pennsylvania. The two hijackers who resided in San Diego, Nawaf al Hazmi and Khalid al Midhar, were part of the conspirators who crashed American Airlines flight 77 into the Penatagon at 9:38am on September 11, 2001. The loss of over three thousand lives that day reminds us of the terrible harm that these fundamental extremists can inflict on our society and its citizens.

We also know that LAX has been targeted by terrorists. As part of what is known as the "Millennium Plot", Mr. Ahmed Ressam, an Algerian national, was intercepted at the Canadian border with a truck load of explosives. He later admitted that he intended to "blow up" the Tom Bradley International Terminal at LAX as part of a simultaneous, multi-national attack targeting sites in Amman, Jordan and a US warship, the USS The Sullivans, in the harbor of Aden, Yemen.

This is the challenge we face - a transnational enemy with whom negotiated peace is not an option. And how many enemies do we have? The US Intelligence Community estimates that 10,000 to 20,000 fighters were trained at Bin Laden supported camps in Afghanistan from 1996 through 2001 while the Taliban regime provided Al Qaeda a sanctuary. We also know our enemy is patient and is willing to return to the same target. For example:

World Trade Center

- Initial bombing in 1993 by Ramzi Yousef - (KSM's nephew)
- 2nd attacks on the World Trade Center was first conceived, according Khalid Sheikh Mohammed, the 9/11 mastermind, as early as 1995.

United States Warships

- January 3, 2000 - attack on The USS The Sullivans fails when raft with explosives sinks.
- October 12, 2000 - al Qaeda operatives ram the USS Cole with a small boat laden with explosives killing 17 and wounding 40.

These incidents and investigations speak volumes about the nature of threats we face. To confront these threats, we have developed systems for a wide variety of homeland security needs to combat terrorism. These include: information sharing and threat assessment; training and exercising programs; critical infrastructure protection; and planning and preparedness tailored to fighting terrorism.

PREVENTING CATASTROPHES

Enhancing Information Sharing

The Schwarzenegger Administration has invested heavily in enhancing California's Terrorism Threat Assessment System. The Governor has emphasized that prevention of a terrorist attack must be our office's number one priority. The plan to detect, deter and prevent terrorism in California is based on public safety partnerships in information sharing, analysis, and investigation support.

These partnerships bring together federal, state and local law enforcement agencies, and their respective law enforcement, public safety and criminal information systems. Our prevention and information sharing strategy incorporates the various initiatives and developments throughout California since 9/11, establishes a statewide structure, and integrates our state and local efforts with our partners in the U.S. Department of Homeland Security, the FBI and other federal law enforcement agencies.

To compliment federal efforts by U.S. Department of Homeland Security and the FBI, California has created four mutually supporting Regional Terrorism Threat Assessment Centers, aligned with the four FBI Field Offices in the state (San Diego, Los Angeles, San Francisco and Sacramento), and a State Terrorism Threat Assessment Center, all linked by a common information sharing system (JRIES).

The State Terrorism Threat Assessment Centers (STTAC) is a partnership of the California Department of Justice, the California Highway Patrol and the California Office of Homeland Security (OHS), with representation including numerous other allied state and federal agencies including, FBI, ICE, USCG, USSS, CA DMV, CDFA, CA Dept of Insurance, CDCR, and OES.

The State Center is designed to provide California's senior leaders with:

- situational awareness of identified threats,
- visibility of and coordination with the critical infrastructure of the state,
- and constant access to the latest local, state and national information analysts products and assessments.

The Center provides:

- statewide assessment products,
- information tracking and pattern analysis,
- geographic reporting linkages
- and connection with the latest national information from the FBI, DHS and other federal agencies.

The STTAC has extensive Geographic Information System (GIS) data on the state's critical infrastructure and potential vulnerabilities, linked to incident reporting by local agencies and the RTTACs to provide a Predictive Indicators Database for our critical infrastructure sites and provide assessments on industry vulnerabilities.

The STTAC monitors identified law enforcement operations throughout California and public sources on international and national events, receives reports from federal, state and local government agencies on events of interest, conducts known terrorist group analysis and is a participant in national reporting and collection systems.

The STTAC provides 24/7 situational awareness for OHS and has direct linkage to the National Counter Terrorism Center and the national watch lists. The STTAC will soon have personnel actually located within the intelligence directorate of the U.S. Department of Homeland Security in Washington DC, complimenting the LAPD officers staffing the DHS Homeland Security Operations Center.

The STTAC has a web-based terrorism-information portal for law enforcement and public safety agencies statewide. Through this secure site, local public safety officials can gain direct access to the entire range of law enforcement sensitive Homeland Security alerts, reports, analysis and daily reporting. Further, this single site will provide a common point of entry for field reports, tips, alerts, and requests for information.

The four Regional Terrorism Threat Assessment Centers (RTTACs) are located in San Diego, Los Angeles, Sacramento and the San Francisco Bay Area, and are generally modeled on the Terrorism Early Warning Group concept pioneered in Los Angeles County and now being recommended by DHS nationwide.

Their areas of responsibility will mirror those of the four FBI Field offices in California, minimizing reporting conflicts, providing statewide coverage and facilitating coordination with the FBI. The RTTACs will be physically co-located with the FBI Joint Terrorism Task Forces (JTTFs). The RTTACs and JTTFs will have mutual information exchanges, through a common communications and collaboration system (JRIES).

The RTTACs will develop a regional threat assessment picture, will have analytical functions and will directly connect to each other and to share information and produce assessments, reports and other threat and warning products. At the local level law enforcement and public safety agencies are designating Terrorism Liaison Officers (TLO) who are trained in the review and assessment of local reporting and in conducting outreach to other public safety agencies, critical infrastructure operators and community groups.

The TLO is the local agency point of contact for all terrorism-related alerts, requests for information, warnings and other notifications from regional, state or federal homeland security agencies. The TLOs review local agency reports, manage local reporting and initiate or respond to requests for information. The TLOs have an ongoing relationship with other local agencies, especially those with daily contact in the community, and develop relationships with critical infrastructure sites within their respective jurisdictions, establishing a personal connection with their security and management staff. Through a single web-based state terrorism website, the TLOs and his or her agency have access to all available terrorisms alerts, notices, information and documents with searchable databases.

Our California system fully compliments and serves the needs of both the FBI and the U.S. Department of Homeland Security, providing access to information from the local police officer to national analyst and investigator, all sharing access to information and sharing relevant products to ensure better safety for our state and nation. Our system is fully compatible with the National Criminal Information Sharing Plan from the U.S. Department of Justice, and our regional information sharing strategy is the largest and most comprehensive in the nation.

Protecting Critical Infrastructure to Prevent and Deter Attacks

Another key component of California's Homeland Security Strategy is the protection of critical infrastructure and key resources. Critical infrastructure and key resource sites are potential terrorist targets deemed most crucial in terms of national-level public health and safety, governance, economic and national security, and public confidence consequences. The critical infrastructure sectors that will ultimately populate the National Asset Database include: agriculture and food; banking and finance; chemical and hazardous materials industry; defense industry base; energy; emergency services; information technology; telecommunications; postal and shipping; public health; transportation; water; and national monuments and icons. Key resources include: commercial assets; government facilities; dams; and nuclear power plants.

California has been selected as the test-bed for a DHS critical infrastructure pilot program called ACAMS – Automated Critical Asset Management System. ACAMS is a secure, interoperable, web-based information database that will allow users to inventory critical assets in their geographical area using the DHS National Asset Database criteria. Most important, this will create a common operating picture across the nation and within DHS

and other law enforcement information analysis agencies. The inventory process will be completed this calendar year, with statewide training to commence in FY06.

To assist local and state public safety agencies secure critical sites, the Congress approved funding for the Buffer Zone Protection Program (BZPP). The BZPP is designed to reduce vulnerabilities of critical infrastructure and key resource sites by extending the protected area around a site into the surrounding community and supporting the prevention and preparedness efforts of local first responders. Funds are used to assist local authorities responsible for protecting and responding to critical infrastructure and key resource sites in an emergency.

Under this program, local law enforcement develops and implements buffer zone protection plans to increase the level of protection and act as a deterrent and prevention mechanism of possible terrorist threats or incidents. In federal fiscal year 2005, California received \$12.9 million.

The 9/11 Commission Report recognizes the difficulty and value of deterring attacks on critical infrastructure sites. The 9/11 Commission found, “In measuring effectiveness, perfection is unattainable. But terrorists should perceive that potential targets are defended. They may be deterred by a significant chance of failure”. We too believe robust security systems will help deter terrorists.

In furtherance of leveraging homeland security resources, our office has also partnered with CREATE – the Center for Risk and Economic Analysis and Terrorism Events, the first university center of excellence funded by the DHS and located on the campus of the University of Southern California. CREATE is providing guidance on where to make the most cost-effective investments in reducing the risk of catastrophic terrorist attacks. In addition, CREATE is using risk-based methods to improve the allocation of funds to fight terrorism. In all of these efforts, partnerships will be the key to our success.

Enhancing Preparedness through Training and Exercising

Another component of the State’s *Homeland Security Strategy* is the statewide Homeland Security Training and Exercise Program. This multi-agency, multi-disciplinary team ensures training and exercises for California’s emergency responders are systematically developed and coordinated to respond and recover from terrorist attacks using weapons of mass destruction. The Exercise Program focuses on a robust annual statewide exercise, Golden Guardian. The 2005 Golden Guardian exercise this past November involved more than 2500 participants representing more than 120 federal, state and local agencies. The scenario involved simultaneous attacks on critical infrastructure at sites in the San Francisco/Oakland Bay Area and State Capitol regions.

The Golden Guardian Exercise Series was first introduced in California in 2004, and has become an annual exercise conducted to coordinate response mechanisms of city, county and state governmental entities, private sector and volunteer organizations in response to potential man-made events and natural disasters. The goal of the Golden Guardian

Exercise Series is to build upon the lessons learned from this and subsequent exercises conducted throughout the nation, as well as real-world events.

The training program also coordinates the States emergency responder training; developing training, ensuring training is properly certified, and tracking those who have been trained. Both programs ensure that the lessons learned from previous exercises are folded back into the next year's exercise objectives and are used to identify new training needs.

Additionally, the training and exercise program receives recommendations and guidance on training curriculum development from the Emergency Response and Advisory Training Committee (ERTAC), which was established by legislation in 2003. Training that is geared at preventing acts of terrorism is a major priority. The Terrorism Liaison Officer program that I previously mentioned will become more effective as more and more first responders receive terrorism awareness training. The goal of the awareness training is to provide a working knowledge of terrorist and criminal extremist groups and individuals, their activities and tactics and how to recognize and report indicators of terrorism and criminal extremism.

The objectives of the awareness training are:

- Enhancing preventative capabilities.
- Recognizing potential terrorist indicators, symbols, and behaviors.
- Recognizing common false documents.
- Recognizing and collecting useful intelligence.
- Knowing when and to whom suspicious information should be reported.

And the topics of awareness training include:

- Terrorism Overview -Differentiate terrorists from traditional criminals and recognize typical terrorist methods of operations and criminal violations.
- Law Enforcement Roles-Identify individual roles and responsibilities in the information sharing process and an overview of the nation's counterterrorism resources at the local, state and federal level.
- Domestic Terrorism
- International Terrorism
- Terrorism Indicators
- Community Partnerships

We are also supporting terrorism awareness training to private security professionals, which will utilize an additional 400,000 people who could observe suspicious activity and may ultimately disrupt terrorist plans.

HOW PLANNING HAS EVOLVED TO COMBAT TERRORISM

Homeland Security Presidential Directive 5, *Management of Domestic Incidents* (HSPD-5)

On February 28, 2003, the President issued Homeland Security Presidential Directive 5 (HSPD-5), *Management of Domestic Incidents*, which directs the Secretary of Homeland Security to develop and administer a National Incident Management System (NIMS). This system provides a consistent nationwide template to enable Federal, State, local and tribal governments and private-sector and nongovernmental organizations to work together effectively and efficiently to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size or complexity, including acts of catastrophic terrorism.

National Incident Management System (NIMS)

The National Incident Management System represents a core set of doctrines, concepts, principles, terminology and organizational processes to enable effective, efficient, and collaborative incident management at all levels. It is not an operational incident management or resource allocation plan. To this end, HSPD-5 requires the Secretary of Homeland Security to develop a National Response Plan (NRP) that integrates Federal government domestic prevention, preparedness, response, and recovery plans into a single, all-discipline, all-hazards plan.

The recently unveiled NIMS system was heavily based on California's preexisting Standardized Emergency Management System (SEMS). The Office of Emergency Services and the Office of Homeland Security undertook an integration effort to create a unified NIMS/SEMS system. First responders throughout California are now trained based on this unified management system that incorporates the protocols of both the state and federal governments.

National Response Plan (NRP)

The National Response Plan is an all-discipline, all-hazards plan that establishes a single, comprehensive framework for the management of domestic incidents. It provides the structure and mechanisms for the coordination of Federal support to State, local, and tribal incident managers and for exercising direct Federal authorities and responsibilities. The NRP assists in the important homeland security mission of preventing terrorist attacks within the United States; reducing the vulnerability to all natural and manmade hazards; and minimizing the damage and assisting in the recovery from any type of incident that occurs.

The National Response Plan was in place prior to Hurricane Katrina. The images of millions of Americans dislocated by this natural disaster will continue to resonate. And we must ask whether this new plan contributed to the bureaucratic processes that delayed the federal response once the city of New Orleans and the state of Louisiana became

overwhelmed. In Congress, the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina is expected to release its findings next month. We look forward to reviewing the results of this investigation and will incorporate the findings into our own plans.

Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, (HSPD-7)

Homeland Security Presidential Directive 7 and the Homeland Security Act of 2002 require the Department of Homeland Security to establish a plan to unify the nation's efforts to protect critical infrastructure and key resources from acts of terrorism. The draft of the full National Infrastructure Protection Plan (NIPP) was released on November 2, 2005. The NIPP provides the framework for conducting operational risk assessment and risk management activities, improving information-sharing and enhancing public-private-sector coordination.

While the final National Infrastructure Protection Plan has yet to be released, California, as mentioned previously, is already working to effectively identify and protect our critical infrastructure. In fact, earlier this month, the Office of Homeland Security convened a critical infrastructure protection strategy session with public safety officials from all levels of government and the private sector. The meeting provided a forum for our federal, state and local partners that are uniquely invested in achieving the goals and objectives set forth in HSPD-7.

We are also in the process of completing a statewide site inventory to populate the Automated Critical Asset Management System (ACAMS) database. California is the first state to do this. We have also entered into an agreement with the federal Protected Critical Infrastructure Information Management Office to implement the PCII program statewide. The Schwarzenegger Administration and legislature also provided an additional layer of security to critical infrastructure with the passage of AB 1495, which protects the sensitive vulnerability and security information furnished by our critical infrastructure owners and operators from public disclosure.

The PCII Program is designed to encourage the private sector to voluntarily share their sensitive vulnerability and proprietary business information with the Federal Government for the purposes of national critical infrastructure protection and planning. California, again, is the first state to do this, in conjunction with ACAMS.

Homeland Security Presidential Directive 8, *National Preparedness*, (HSPD-8)

The National Preparedness Directive issued on December 17, 2003, tasked the Secretary of Homeland Security, in coordination with the heads of other appropriate Federal departments and agencies and in consultation with State and local governments, to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters and other emergencies. It requires: 1) a national domestic preparedness goal; 2) mechanisms for improved delivery of Federal

preparedness assistance to State and local governments; and 3) actions to strengthen preparedness capabilities of Federal, State and local entities.

The National Preparedness Goal

The National Preparedness Goal establishes a vision, capabilities, and priorities for national preparedness. It will be utilized in conjunction with the following three capabilities-based planning tools: the National Planning Scenarios, Universal Task List (UTL), and Target Capabilities List (TCL). Collectively, they identify key requirements that can help guide domestic all-hazards preparedness efforts. These documents define critical tasks that must be performed during a major event to reduce the loss of life, mitigate significant property damage and recover from disasters. They also identify core capabilities we need to achieve and sustain as a Nation and, therefore, will transform how the Federal government proposes to invest in homeland security missions.

The vision of the National Preparedness Goal is to engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy.

National Planning Scenarios

A range of scenarios developed by a Federal interagency working group led by the White House Homeland Security Council were used to illustrate the potential scope, magnitude, and complexity of incidents of national significance. The 15 National Planning Scenarios, which include both terrorism and natural disasters, provided parameters regarding the nature and scale for incidents of national significance and the basis to define prevention, protection, response and recovery tasks that need to be performed, as well as the capabilities required to perform them. The National Planning Scenarios represent a range of potential incidents, rather than every possible threat or hazard. Developing the national capacity to prevent, protect against, respond to, and recover from these challenges will create the agility and flexibility required to meet a wide range of threats and hazards.

The 15 National Planning Scenarios are:

- | | |
|------------------------------|---------------------------------|
| 1. Improvised Nuclear Device | 9. Major Earthquake |
| 2. Aerosol Anthrax | 10. Major Hurricane |
| 3. Pandemic Influenza | 11. Radiological Device |
| 4. Plague | 12. Improvised Explosive Device |
| 5. Blister Agent | 13. Food Contamination |
| 6. Toxic Industrial Chemical | 14. Foreign Animal Disease |
| 7. Nerve Agent | 15. Cyber |
| 8. Chlorine Tank Explosion | |

Universal Task List

Nationally representative teams identified tasks required by each of these scenarios. These tasks have been combined into a comprehensive menu called the Universal Task List (UTL). The UTL is designed to serve as a common language and reference system, as the foundation for learning and exercising objectives, as a tool for operational planning, and for use in evaluations and assessments of performance. Tasks are identified that need to be performed by all levels of government and a variety of disciplines for an incident of national significance. No single jurisdiction or agency is expected to perform every task. Rather, subsets of tasks will be selected based on specific roles, missions, and functions. There are approximately 1,600 tasks encompassing all levels of government and disciplines from the national strategic to the incident level.

Target Capabilities List

As the heart of the National Preparedness Goal, the Target Capabilities List (TCL) provides guidance on the specific capabilities and levels of capability that Federal, State, local and tribal entities will be expected to develop and maintain. Entities will not be expected to develop and maintain every capability to the same level. The specific capabilities and levels of capability will vary based upon the risk and needs of different types of entities.

This fiscal year, the U.S. Department of Homeland Security has identified eight national capability priorities. They are: information sharing and dissemination, law enforcement investigation and operations, interoperable communications, CBRNE (Chemical, biological, radiological, nuclear, explosive) detection, WMD/hazardous material response and decontamination, mass prophylaxis and medical surge capacity.

FY 2006 HOMELAND SECURITY GRANT PROGRAMS

These homeland security presidential directives and national plans will have a major impact on the amount of funds California will receive in federal preparedness dollars. Federal Fiscal Year 2006 marks the first grant cycle in which the National Preparedness Goal and the National Priorities are in place. The Department of Homeland Security has integrated the Goal and the National Priorities into the FFY 2006 grant programs.

Funding for the State Homeland Security Program, and the UASI, and Law Enforcement Terrorism Prevention Program (LETPP) will be allocated on risk and need. Risk will be assessed at the federal level using two risk calculations: asset-based terrorist risk and geographically-based terrorist risk. These risk calculations are summed to produce a total terrorism risk score.

The competitive portion of the FY2006 application will be the development of a statewide enhancement Plan and Investment Justifications from the state as well as from each of five federally designated high-risk urban areas to determine how well we have

invested homeland security dollars; identify areas that are strengths and weaknesses; and identify how funds should be used to fill gaps in preparedness.

To prepare for the FFY 2006 application process, the Office of Homeland Security gathered over 200 public safety officials from across the state to attend a three-day program capabilities review workshop earlier this month. With this vast amount of experience from California's first responders, the Office of Homeland Security will work with our local and state partners to determine the capabilities of the state and local jurisdictions to prevent, protect, respond to and recover from a catastrophic event. Essentially, we asked local and state jurisdictions to identify where they are, where they needed to be, and how they planned on filling the gap.

Based upon the Program Capabilities Review conference, the OHS will develop an enhancement plan and an investment justification plan on behalf of the state. The enhancement and investment justification plan will be reviewed by the US Department of Homeland Security to determine allocations of federal preparedness grants. These plans will also guide additional homeland security investments throughout the state and make all of our communities better prepared to prevent, protect, respond to and recover from natural catastrophes and acts of terrorism.

CONCLUSION

We live in a high risk state. California is an attractive target for acts of terrorism and we can plan on natural disasters occurring with regularity. The images from the 9/11 attacks and Katrina continue to resonate and remind us that we must plan and prepare for catastrophic events. Public safety is the Governor's highest priority. While much has been accomplished, much will always remain to be done. We will continue to work harder each day to improve our ability to prevent a potential terrorist attack and improve our preparedness, response and recovery capabilities across the State and the Nation.

I greatly appreciate the opportunity to share with you some of the work of the dedicated professionals involved with homeland security and I look forward to discussing these efforts with the Commission.

Encl: California Homeland Security Strategy