

Statement by  
Honorable Paul McHale,  
Assistant Secretary of Defense for Homeland Defense

Before the 109<sup>th</sup> Congress  
Subcommittee on Terrorism, Unconventional Threats and Capabilities  
Committee on Armed Services  
United States House of Representatives

March 15, 2005

## **Introduction**

Chairman Saxton, Congressman Meehan, distinguished members of this Subcommittee: Thank you once again for inviting me back to address the progress we have made in improving the defense of the United States.

Defense of the United States requires a comprehensive understanding of the global threat. A successful defense of the United States homeland is the preeminent requirement of the Global War on Terrorism. There is no “home game.” There is no “away game.” We are engaged in a global conflict. And in that global conflict, the defense of the U.S. homeland is the preeminent duty.

Therefore, Homeland Defense must be seen as an integral part of a global, active, layered defense – a defense in depth – that has as its single goal to secure the United States and its citizens from attack.

As the President explained during the State of the Union address, “Our nation, working with allies and friends, has also confronted the enemy abroad, with measures that are determined, successful, and continuing. The al Qaeda terror network that attacked our country still has leaders -- but many of its top commanders have been removed. There are still governments that sponsor and harbor terrorists -- but their number has declined. There are still regimes seeking weapons of mass destruction -- but no longer without attention and without consequence. Our country is still the target of terrorists who want to kill many, and intimidate us all -- and we will stay on the offensive against them, until the fight is won.”

Our strategic approach of necessity involves multiple fronts, not just different geographical theaters; not even primarily military fronts. This struggle is not just about stopping and capturing terrorists, although that is critically important. The main elements of the U.S. strategy in the global

war on terrorism are: (1) protecting the homeland; (2) disrupting and attacking terrorist networks; and (3) countering ideological support for terrorism. The third – the ideological fight – we see as the key to victory.

Like the Cold War before it, the Global War on Terrorism will be the work of a generation. The task of defending freedom now falls to us and, like every generation of Americans that has gone before, we do not shrink from that responsibility, but embrace it.

### **DoD's Role in the Security of Our Nation**

This global war involves all elements of America's power; military force plays a critical, but by no means exclusive, role. Indeed, the various instruments of our national power, including intelligence, law enforcement and diplomacy, for example, serve to reinforce one another. For instance, the Department of the Treasury's interdiction of financial support lines chokes off vital resources terrorist networks need to plan and execute attacks against our forces our homeland, or against our allies. Moreover, the President's Proliferation Security Initiative has forged a partnership of nations to interdict by legal, diplomatic, economic, military or other means the flow of weapons of mass destruction, their delivery systems, and related materials. Here at home, the Department of Homeland Security (DHS) is protecting our nation's borders, ports, and territorial seas, working with the public and private sectors to reduce our vulnerabilities, and preparing our nation to respond quickly and decisively to terrorist attacks. At the same time, the Federal Bureau of Investigation (FBI) is apprehending suspected terrorists who have penetrated our borders.

The contribution of the U.S. military has been indispensable to the successes we have achieved so far. DoD has the lead in providing for the defense of the United States and is an important government partner in providing for homeland security. Defense responsibilities range from overseas military missions to planning for Homeland Defense under my supervision as the Assistant

Secretary of Defense for Homeland Defense and under the auspices of the Commander, U.S. Northern Command (USNORTHCOM), and the Commander, U.S. Pacific Command (USPACOM). At the direction of the President or the Secretary of Defense, DoD will undertake military missions at home to defend the United States, its population, and its infrastructure from attack.

Some have asserted that the distinctions between “Homeland Defense” and “homeland security” are “artificial” and “impractical,” but such assertions could not be further from historic truth.

The distinctions between the role of DoD and those of DHS, the Department of Justice (DOJ), and other government agencies responsible for the domestic security of the United States are not “artificial” or “impractical,” but rather are complementary and consistent with the law and operational requirements. The Homeland Security Act of 2002, Section 876, provides that nothing in the Act confers upon the Secretary of the Department of Homeland Security any authority to engage in “warfighting, the military defense of the United States, or other military activities.”

This year we will complete the first strategy for the Department’s Homeland Defense mission. This new Homeland Defense and Civil Support Strategy defines strategic goals for the Department’s role in Homeland Defense and civil support. By providing strategic goals and objectives, we add coherence and direction to the disparate activities across the Department that include deterring and preventing attacks, protecting critical defense and designated civilian infrastructure, providing situational understanding, and preparing for and responding to incidents.

In addition to taking the fight to our adversaries abroad, DoD is postured to deter, defend against, and defeat external and other direct threats to the United States:

**Air Domain.** The air domain is guarded, patrolled, and monitored by the binational U.S.-Canada North American Aerospace Defense Command (NORAD). On a daily basis, the men and women of the United States Air Force, United States Air Force Reserve, and the Air National Guard secure the skies over major metropolitan areas, and our nation's critical infrastructure. Since September 11, 2001, more than 39,500 fighter, aerial refueling, and airborne early warning sorties have been flown in defense of the United States, while more than 1,900 fighter air patrols have responded to unknown aircraft and other suspicious flight operations.

**Maritime Domain:** The maritime domain – including international waters, the sea approaches to the United States, our territorial seas, and other U.S. navigable waters – are guarded by a dynamic and highly effective partnership between the U.S. Navy and the U.S. Coast Guard. The U.S. Navy defends the sea approaches to the United States and works with the U.S. Coast Guard to patrol international waters and our territorial seas. Under the auspices of Maritime Homeland Defense operations, naval maritime surveillance and interdiction forces are designated for transfer to the command and control of Commander, USNORTHCOM, when directed by the Secretary of Defense.

Additionally, in multiple theaters in the global war on terror, the Navy is conducting Maritime Interception Operations (MIO) to deter, delay and disrupt the movement of terrorists and terrorist-related materials at sea before they can reach our shores. Over the course of the last year, the Navy monitored, queried and boarded merchant vessels some 2,200 times.

**Land Domain:** DHS, as noted earlier, is responsible for protecting our nation's borders, ports, and territorial seas, working with the public and private sectors to reduce our vulnerabilities, and preparing our nation to prevent, or if necessary, quickly and decisively respond to terrorist attacks. DOJ, the FBI, and, indeed, the entire law enforcement community – at Federal, State, and local levels

– are working to identify, track, and capture terrorists who may have penetrated our nation’s borders. In these activities, DoD’s role is to provide support to civil authorities, when appropriate and as permitted by law.

Beyond assisting law enforcement missions, DoD is ready to defend the United States directly. DoD has postured numerous assets both to defend the U.S. homeland and to assist civil authorities:

- Quick Reaction Forces and Rapid Reaction Forces, highly trained U.S. Army and U.S. Marine Corps units, are postured to respond to a wide range of potential threats to the U.S. homeland. When deployed, these forces will operate under Commander, USNORTHCOM, and Commander, USPACOM, command and control.
- Joint Task Force Civil Support, headquartered in Fort Monroe, Virginia; Joint Task Force Consequence Management East, headquartered at Fort Gillem, Georgia; or Joint Task Force Consequence Management West, headquartered at Fort Sam Houston, Texas; under the command and control of Commander, USNORTHCOM, can provide consequence management support to civil authorities in the case of weapons of mass destruction attacks.
- Joint Force Headquarters National Capital Region, based at Fort McNair in Washington, DC, is responsible for land Homeland Defense, civil support, and consequence management in the National Capital Region.
- Joint Task Force North, headquartered at Fort Bliss, Texas, supports counterdrug, counterterrorism, and other operations to counter transnational threats.

- Joint Task Force Alaska, based at Elmendorf Air Force Base, Alaska, is responsible for land Homeland Defense and civil support operations in Alaska.
- Joint Task Force Homeland Defense, based at Fort Shafter, Hawaii, is responsible for land Homeland Defense and civil support in Hawaii and U.S. territories, possessions, and protectorates in the Pacific.

DoD uses the Total Force concept – the right forces for the right jobs – to execute its missions. The Total Force – Active, Reserve, and National Guard – is even now engaged in activities at home and abroad that promote the security and interests of our nation.

The National Guard, in particular, provides unique capabilities in every U.S. State and territory. The modern-day National Guard effectively operates as an operational force for military missions at home and abroad and can answer no-notice calls by the President, the Secretary of Defense, or the governors to respond to natural or man-made catastrophic incidents here at home.

The National Guard provides important capabilities to USNORTHCOM and USPACOM, including situational awareness capabilities, intelligence and information feeds, chemical-biological weapons of mass destruction response force packages, and forward-deployed command and control apparatuses and joint logistics bases, as needed.

Also, the Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005 authorized the Secretary of Defense to provide funds to the Governor of a State for the use of the National Guard in a Title 32 Status (State control/Federal funding) for approved Homeland Defense activities. This new authority recognizes both the truly global nature of the current war and the special capabilities and contributions of the National Guard, a force located in every State

and territory; very familiar with the local geography, officials, and population; and well versed in working with other U.S. agencies. Under this new Secretary of Defense authority, National Guard forces will be engaged directly in the defense of the homeland in a manner not seen since the early days of our country.

### **Role of DoD and Other Agency Exercises**

DoD is committed to maintaining the readiness of military forces to execute the full spectrum of Homeland Defense operations and to support civil authorities, when appropriate. To this end, DoD has hosted or participated in our own exercises and those sponsored by other government entities.

Homeland security and Homeland Defense exercises are critical to ensuring readiness and identifying gaps and potential weaknesses within each agency and across agencies in responding to terrorist attacks, including multiple, simultaneous challenges. These exercises support the DHS National Homeland Security Exercise Program established by Homeland Security Presidential Directive-8 (HSPD-8), National Preparedness (December 17, 2003). Since my last testimony, these exercises have included: Scarlet Shield (May 2004); UNIFIED DEFENSE (February 2004); Dark Portal (February 2004); and DETERMINED PROMISE (August 2004).

This year, DoD will continue to host and participate in these very worthwhile exercises. Senior DoD civilian and military personnel, for example, will participate in numerous national-level tabletop exercises such as the Senior Officials Exercises and Top Officials (TOPOFF) III, which will be held in April 2005. USNORTHCOM's UNIFIED DEFENSE and DETERMINED PROMISE exercises will be held again this year under the new names ARDENT SENTRY and VIGILANT SHIELD, respectively. Additionally, as it has for the last three and a half years, NORAD will continue to execute periodic air defense exercises to ensure our forces are effectively postured to detect, deter and, if necessary, defeat hostile aircraft operating in U.S. and international airspace.



## **DoD Support of Critical Infrastructure Protection**

Public Law 107-296 (the Homeland Security Act of 2002) assigned DHS the responsibility to develop a comprehensive national plan to protect our nation's critical infrastructure and key assets. The National Strategy to Secure Cyberspace (February 2003) and the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets (February 2003), as well as HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection (December 17, 2003), designated DoD as the Sector Specific Agency for the Defense Industrial Base sector. This designation recognizes DoD's important role in the protection of the nation's critical infrastructure that sustains our capability to defend our nation and fight its wars. In this capacity, DoD must work closely with private sector owners of critical defense infrastructure to deter, mitigate, or neutralize terrorist attacks in order to sustain military operations.

As I testified last year, in 2003 I was assigned the responsibilities for Defense Critical Infrastructure Protection and DoD's efforts in ensuring the protection of the Defense Industrial Base sector. Protecting Defense Critical Infrastructure is essential to ensuring the mission readiness of our military forces to protect the United States and to project power globally. Just as important is the protection of the Defense Industrial Base sector, which is the source of mission essential components, ordnance, and other equipment.

We have registered much progress to date. For example, Commander, USNORTHCOM, and Commander, USPACOM, now include Defense Critical Infrastructure and the Defense Industrial Base in their operational planning.

Further, in 2004, my office evaluated the Defense Industrial Base sector and identified 148 critical assets. We then conducted vulnerability assessments of 66 key sites where these critical assets are produced. DoD shared with DHS the results of this evaluation and the supporting assessments. To improve the protection of these sites and others, we developed a Defense Infrastructure Sector

Assurance and Mission Assurance Plan and are currently developing a web-based tool to help industries of the Defense Industrial Base assess their own vulnerabilities. In addition, in collaboration with the Adjutants-General of the States, we have conducted vulnerability assessments and, where appropriate, assisted in identifying measures to reduce vulnerabilities. We have also shared Defense Industrial Base information with 14 States at their request.

This year we expect to conduct more in-depth, comprehensive vulnerability analyses of the 148 critical assets, develop recommended measures for the sector to eliminate key vulnerabilities, and complete development of the web-based self-assessment tool. We will again share the results of our work with both DHS and the States.

### **Intelligence and Information Sharing**

As President Bush stated on December 17, 2004, as he signed into law the Intelligence Reform and Terrorism Prevention Act of 2004, “America, in this new century, again faces new threats. Instead of massed armies, we face stateless networks; we face killers who hide in our own cities. We must confront deadly technologies. To inflict great harm on our country, America's enemies need to be only right once. Our intelligence and law enforcement professionals in our government must be right every single time. Our government is adapting to confront and defeat these threats.”

DoD works closely with the Intelligence Community to maintain maximum awareness of threats to the United States. My office works closely with the Under Secretary of Defense for Intelligence (USD(I)), established by the Bob Stump National Defense Authorization Act for Fiscal Year 2003, on all Homeland Defense and homeland security matters. USD(I) is charged with ensuring that the senior DoD leadership receives the warning, actionable intelligence, and counter-intelligence support needed to pursue the objectives of the National Defense

Strategy, including defense of the homeland. USD(I) also provides a single point of contact for coordination of national and military intelligence activities.

With the assistance of my office, the Office of the Under Secretary of Defense for Intelligence is working with DHS and other Federal departments and agencies to meet the requirements of Executive Order 13311, *Homeland Security Information Sharing* (July 2003), to establish procedures for the horizontal sharing of information among Federal agencies and the vertical sharing of information with authorities at State and local levels, and with Executive Order 13356, *Strengthening the Sharing of Terrorism Information To Protect Americans* (August 2004), to maximize the secure interchange of terrorism information between agencies and appropriate State and local authorities.

Since its establishment in May 2003, DoD has been a full partner in the Terrorist Threat Integration Center (TTIC) – now integrated by direction of the Intelligence Reform and Terrorism Protection Act of 2004 into the National Counterterrorism Center. DoD is also a partner in the Terrorist Screening Center (TSC), which was established by Homeland Security Presidential Directive – 6, *Integration and Use of Screening Information* (September 16, 2003), to consolidate terrorist watchlists and provide 24/7 operational support for thousands of aviation screeners across the country and around the world.

In July 2004, the Secretary of Defense approved the sharing of biometric (e.g., fingerprints, photographs) and biographical data collected from enemy prisoners of war with other Federal departments and agencies. DoD has more than 100,000 records containing biometric information on persons of interest from the Persian Gulf War, Operation ENDURING FREEDOM in Afghanistan, and Operation Iraqi Freedom in Iraq. Although many of the details are very sensitive, we have had a number of successes based on sharing this data.

The Defense Intelligence Agency's (DIA's) Joint Intelligence Task Force-Combating Terrorism (JITF-CT) is DoD's lead national-level intelligence

organization for indications and warning, the production of timely all-source intelligence, integration of national-level analytic efforts on all aspects of the terrorist threat, and development and maintenance of an accurate, up-to-date knowledge base of terrorism-related information. JITF-CT shares this threat information and knowledge base throughout DoD, and with the Intelligence Community, law enforcement agencies, and DHS. Last year, JITF-CT provided to DHS the automated information sharing system, now called the Homeland Security Information Network (HSIN), to facilitate information sharing among intelligence (Federal, State, and local) and law enforcement entities.

DIA products and activities -- in addition to terrorism analysis -- that support the homeland security mission are routinely shared with DHS and its component organizations. Examples include: cyber threat warning assessments; human factors and social network analyses; nuclear, chemical and biological threat analyses; counterdrug analyses; broad, integrated Homeland Defense threat assessments with a ten-year horizon; assessments of specific missile threats to aircraft; assessments of potential release of toxic chemicals from industry along the Canadian and Mexican borders; medical intelligence assessments; and analyses of emerging technology threats to homeland security.

Finally, partnering with the U.S. Coast Guard, DoD has established the Maritime Domain Awareness Senior Steering Group to develop an enhanced capability to identify threats to the maritime domain as early and as distant from our shores as possible by integrating intelligence, surveillance, observation, and navigation systems into a common operating picture accessible throughout the U.S. Government.

### **DoD Relationship with the Department of Homeland Security**

DoD and DHS work in close coordination to ensure the safety and security of the U.S. Homeland. Coordination and cooperation take place continuously at all levels of both organizations.

As the Secretary of Defense's principal representative to DHS, I have worked diligently to build upon and improve our excellent working relationships throughout DHS. In 2003, DoD and DHS signed a memorandum of agreement that authorized detailing some 64 DoD personnel to DHS to fill critical specialties, principally in the areas of communications and intelligence. DoD continues to maintain a 24/7 presence in the DHS Homeland Security Operations Center (HSOC), provide planning teams, when needed, for the DHS Interagency Incident Management Group – a group of senior Federal department and agency officials focused on incident response – and provide a DoD advisory and liaison office within DHS headquarters: the Homeland Defense Coordination Office.

A key accomplishment since my last appearance was publication of the National Response Plan in December 2004. DoD supported DHS, along with other Federal departments and agencies, in integrating existing Federal response plans (e.g., Federal Response Plan, Interagency Domestic Counter-Terrorism Concept of Operations, National Contingency Plan, and the Federal Radiological Emergency Response Plan), in accordance with the Homeland Security Act of 2002. The resulting single, national all-hazards incident plan is a testament to the dedication and hard work of countless individuals who have contributed tangibly to preparing our nation for the full range of man-made and natural emergencies.

Perhaps as significantly, DoD supported DHS's development and execution of an Interagency Security Plan to address heightened terrorist threats following the March 2004 Madrid train bombing. In support of the Interagency Security Plan, DoD supported:

- Joint Task Force WINTER FREEZE. Initiated on November 2, 2004, under the Operational Control of Joint Task Force North (JTF-N) and Commander, USNORTHCOM, Operation WINTER FREEZE supported DHS, Customs and Border Patrol, with interdiction of suspected transnational threats along the

U.S./Canadian border in New Hampshire, Vermont, and New York. JTF-N is credited with assisting in the interdiction of forty-seven Special Interest Aliens in the Border Patrol's Buffalo, Swanton, and Houlton sectors and with gathering information about the Ali, Shah, and Galdamez alien smuggling organizations.

- Aviation Security Vulnerability Assessments. Six Defense Threat Reduction Agency (DTRA) personnel supported the Transportation Security Agency (TSA) at Boston Logan Airport to train TSA personnel in the conduct of an airport site survey to obtain a security measures baseline.
- Improvised Explosive Device (IED) Detection Training. Approximately four personnel from the Department of the Army's Vehicle-Borne IED Task Force provided detection training to DHS inspectors.
- Surface Transportation Vulnerability Assessment. Surface Deployment Distribution Command maintained a three-person assessment team on standby to perform surface transportation vulnerability assessment assistance to DHS.
- Two Forward Surgical Teams (FSTs), a total of 41 personnel, provided support for one week prior to and following the Presidential Election and Inauguration. Army Forces Command maintained the two FSTs in a 48-hour deployment posture, while U.S. Transportation Command maintained an alert posture to support short-notice movement of the teams.
- Six National Guard personnel and two Mobile Vehicle Inspection System vehicles were prepared to deploy, if requested by DHS.

- Four DTRA personnel were prepared to deploy to provide technical support and a command and control element to provide radioisotope detection and identification in 11 major airports. The DTRA personnel were prepared to deploy on order to train and equip approximately 30 Transportation Security Agency personnel to screen, locate, and identify radiological materials.

DoD is currently engaged in supporting DHS in its development of the 2005 Interagency Security Plan. To date, we have reviewed 151 DHS mission area initiatives and provided recommendations on potential DoD contributions.

As it did in 2003, DoD provided unmanned aerial vehicle (UAV) support to DHS in 2004. From June 18 to September 30, 2004, DoD provided Hermes 450 UAVs to DHS in support of the Arizona Border Control Initiative (ABCI). The ABCI sought to detect and identify suspicious activities at the Arizona border (e.g., illegal entry, smuggling activity, and/or drug activity) and aid in rescuing lost or injured persons. The Hermes 450 flew 590.1 hours and is credited with 1,678 detections, leading to 965 apprehensions, and the seizure of 843 pounds of marijuana. From November 3, 2004, to January 24, 2005, DoD provided Hunter UAVs to DHS in support of the ABCI. The Hunter logged 287.6 hours and is credited with 456 detections, leading to 287 apprehensions, and the seizure of 1889.81 pounds of marijuana.

DoD also assisted the U.S Coast Guard in evaluating sensors and platforms that will enhance their ability to conduct wide area surveillance to detect, identify, and track vessels of interest. To this end, the U.S Coast Guard has explored long-range radar systems, UAVs, and High Altitude Long Endurance and Lighter than Air airships.

Finally, DoD is working with DHS and the other interagency partners, including the Department of State and the FBI, to establish the Domestic Nuclear Detection Office (DNDO). DoD, through its participation in the DNDO, will assist

in the development of the global nuclear detection architecture, ensure that a detection and reporting system is standardized, provide systems engineering expertise, and work to create effective and efficient interfaces across Federal, State and local levels.

### **DoD Relationship with the Homeland Security Council**

In my capacity as the Assistant Secretary of Defense for Homeland Defense, I am DoD's principal representative to the Homeland Security Council (HSC) staff and represent DoD at HSC principals and deputies committee meetings when the Secretary of Defense or Deputy Secretary of Defense are unable to participate. My office represents DoD on the HSC's interagency policy coordination committees and subordinate working groups, with the participation of other DoD offices as appropriate.

Over the course of 2004, DoD has supported HSC initiatives to improve our national aviation security, information sharing, nuclear power plant security, and biodefense, and to reduce our nation's airports' vulnerability to man-portable air defense systems and our nation's borders to penetration by terrorists. We have also participated in the development of a wide array of presidential directives, including: implementing recommendations of the 9/11 Commission; defense of the agriculture and food system against terrorist attacks, major disasters, and other emergencies; biodefense; enhancing terrorist-related screening through comprehensive, coordinated procedures that detect, identify, track, and interdict people, cargo, conveyances, and other entities and objects that pose a threat to homeland security; establishing common identification standards for Federal employees and contractors; and improving maritime security.

The HSC was also instrumental in coordinating interagency planning to enhance the protection of our nation leading up to and during the 2004 elections and during the 2005 Presidential Inauguration.



## **Defense Support of Civil Authorities**

DoD has continued its long tradition of support to domestic civil authorities while maintaining its primary mission of fighting and winning the nation's wars. Since my last testimony before this Subcommittee, DoD has continued to provide assistance to civil authorities when their resources were overwhelmed or when faced with challenges necessitating the utilization of the Department's unique capabilities.

There are three primary mechanisms by which DoD would take part in a Federal response to a domestic incident. Federal assistance, including assistance from DoD, would be provided: (1) at the direction of the President; (2) at the request of another Federal agency under the Economy Act, or (3) in response to a request from DHS's Federal Emergency Management Agency under the Stafford Act. The second and third mechanisms require a request for assistance and approval of the Secretary of Defense.

First, under the Constitution, the President may direct any Federal agency to provide assets in support of an incident response. The President has the authority to direct any Federal agency, with or without reimbursement, to support state and local assistance efforts in a major disaster or emergency.

Second, another Federal agency can request DoD support in accordance with the Economy Act for non-Stafford Act responses. If DoD assistance is contemplated, the requesting Federal agency submits a request for assistance through the Office of the Secretary of Defense, Executive Secretary. The request is processed through the Joint Staff and Office of the Secretary of Defense and submitted to the Secretary of Defense for a decision.

Lastly, DoD assistance may be requested under the Stafford Act. The requesting Federal agency submits a request for assistance through the Office of the Secretary of Defense, Executive Secretary. The request is processed through

the Joint Staff and Office of the Secretary of Defense and submitted to the Secretary of Defense for a decision.

Once DoD resources are employed in support of domestic civil authorities, they are under the command and control of Commander, USNORTHCOM, for responses in the Continental United States, Alaska, the Commonwealth of Puerto Rico, U.S. Virgin Islands, and the District of Columbia; or Commander, USPACOM, for Hawaii and U.S. territories, possessions, and protectorates in the Pacific region.

An important tenet of defense support of civil authorities is that DoD is always in support of domestic civil authorities. It is also important to note that the chain of command always runs from the President to the Secretary of Defense to the Combatant Commander concerned. The Department fully supports the Incident Command System of the National Incident Management System. However, at no time does the supported agency exercise any command and control over DoD forces.

In addition to the support provided to DHS cited earlier in my testimony, DoD acted on 99 requests for assistance from domestic civilian agencies, including DHS, DOJ, and the National Interagency Fire Center in 2004. For example, DoD provided emergency support to response and recovery operations in Southern Florida for hurricanes Charlie, Frances, Ivan, and Jeanne; wildland firefighting operations in Arizona, California, Nevada, New Mexico, Utah, and Washington; and security support to the G8 Summit, the Democratic and Republican National Conventions, the U.N. General Assembly, and the Presidential Election and Inauguration.

## **Conclusion**

Throughout our history, U.S. military forces – active duty, Reserves and National Guard -- have defended our nation against its enemies on land, at sea, and

in the air, adapting continuously to engage threats to our nation. Today we must cope not only with the threats produced by the proliferation of weapons of mass destruction and missile technology among nation-states, but also with threats posed by individual terrorists and terrorist networks with global reach.

As the 9/11 Commission noted in its final report: “America can be attacked in many ways and has many vulnerabilities. No defenses are perfect. But risks must be calculated; hard choices must be made about allocating resources. Responsibilities for America’s defense should be clearly defined. Planning does make a difference, identifying where a little money might have a large effect. Defenses also complicate the plans of attackers, increasing their risks of discovery and failure. Finally, the nation must prepare to deal with attacks that are not stopped.”

Mr. Chairman, I commend you and the members of the Subcommittee for your continued interest in and support of the Department’s Homeland Defense mission. The citizens of this nation, its institutions, and our brave men and women in uniform have repeatedly demonstrated the patriotism, toughness, innovation, determination, and resiliency to defeat our enemies while retaining our freedoms. There is no doubt in my mind that those capabilities will be tested against this newest enemy threat – nor is there any doubt of our inevitable triumph.

As President Roosevelt stated in his Pearl Harbor Speech on December 8, 1941, “There is no blinking at the fact that our people, our territory and our interests are in grave danger. With confidence in our armed forces - with the unbounding determination of our people - we will gain the inevitable triumph.”