STATEMENT FOR THE RECORD

MICHAEL CHERTOFF

SECRETARY
UNITED STATES DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

UNITIED STATES SENATE
HOMELAND SECURITY AND GOVERNMENT AFFAIRS COMMITEE

"CONFRONTING THE TERRORIST THREAT TO THE HOMELAND:
SIX YEARS AFTER 9/11"

SEPTEMBER 10, 2007

INTRODUCTION

Thank you, Chairman Lieberman, Ranking Member Collins, and Members of the Committee for the invitation to appear today. I appreciate this Committee's steadfast support for the Department and your many actions to improve our effectiveness.

At the outset, I'd like to acknowledge the strong working relationships we share with the Director of National Intelligence (DNI), the Federal Bureau of Investigation (FBI), and the National Counterterrorism Center (NCTC), as well as many other federal, state, and local partners working around the clock to protect our country and the American people from terrorist attacks.

None of us alone can keep our nation safe from the threat of terrorism. Protecting the United States is a mission we share and one that requires joint planning and execution of our counterterrorism responsibilities; effective information collection, analysis, and exchange; and the development of integrated national capabilities.

Of course, tomorrow marks the six-year anniversary of the 9/11 attacks. As our nation remembers this unconscionable act of terrorism and the murder of nearly 3,000 innocent men, women, and children, it is appropriate that we take a moment to assess the current terrorist threat facing our country, weigh our efforts to defend the United States against additional attacks, and set our priorities for the future.

It is no accident that we haven't suffered a major terrorist attack on U.S. soil since 9/11. I believe it is the result of the President's leadership, this Committee's support, and the hard work and constant vigilance of hundreds of thousands of men and women – including the 208,000 employees of the Department of Homeland Security – who are working tirelessly both at home and overseas to protect our country.

Since 9/11, our nation has put in place critical tools that have strengthened our ability to identify terrorist threats to our homeland, dismantle terrorist cells and disrupt terrorist plots, and prevent terrorists from crossing our borders or assuming false identities to carry out attacks.

Among other successes, we foiled serious terrorist plots to attack U.S. military personnel at Fort Dix, New Jersey, and a plot to explode fuel pipelines at John F. Kennedy Airport in New York City. In August of 2006, we also worked with British authorities to disrupt a threat that would have killed thousands of Americans aboard commercial aircraft departing the United Kingdom.

But while we have successfully raised our barrier against terrorist attacks, the fact remains that we are still a nation at risk. The recently issued National Intelligence Estimate makes clear that we continue to face a persistent threat to our homeland over the next several years. We also cannot discount the danger posed by homegrown terrorists, isolated individuals or groups that initiate their own plots after becoming radicalized.

Our nation faces a set of important choices. How do we respond to this ongoing threat? What actions are necessary to protect our country? And how do we build upon our success to date?

OUR DEPARTMENT'S ROLE

As you know, DHS was created to unify and coordinate federal, state, and local capabilities to prevent, protect against, and respond to all hazards – including terrorist attacks.

Congress gave us broad authorities under the Homeland Security Act of 2002 to prevent terrorist attacks in the United States, reduce our nation's vulnerability to terrorism, and assist in the response to and recovery from major attacks. The Intelligence Reform and Terrorism Prevention Act of 2004 also strengthened our ability to share intelligence, improve information sharing and first responder communications, and enhance border and transportation security. Among its key initiatives, the law established the requirement for a secure document to enter or re-enter the United States. We continue to make progress in implementing this key recommendation of the 9/11 Commission. We also have benefited tremendously from the SAFE Ports Act of 2006, which formalized efforts to enhance port security, improve cargo inspections, and strengthen radiation detection, among others.

We recognize that we cannot protect every person from every threat at every moment. To do so would require unlimited resources and would be at a tremendous cost to our freedoms, our economy, and our way of life. Our challenge is to manage risk consistent with our understanding of threats, vulnerabilities, and consequences, and then prioritize our resources to protect against high-threat, high-consequence events.

Since becoming Secretary, I have set five major goals to focus our Department's efforts on a core set of objectives. These goals are as follows: 1) keeping dangerous people from entering our country; 2) keeping dangerous cargo out of our country; 3) protecting critical infrastructure; 4) boosting emergency preparedness and response; and 5) strengthening DHS integration and management.

Because the focus of this hearing is threats to our homeland, my testimony will highlight only the first three goals: preventing dangerous people and dangerous cargo from entering our country, and protecting critical infrastructure. I will also discuss our efforts to share information and intelligence necessary to achieve these goals. I will reserve a discussion of emergency preparedness and the Department's internal management functions for a subsequent hearing. In addition, I testified on these issues last week before the House Committee on Homeland Security.

PROTECTING AGAINST DANGEROUS PEOPLE

A key priority for our Department remains keeping dangerous people from entering the United States to engage in criminal activity or to carry out terrorist attacks. If we can

prevent dangerous people from infiltrating our borders then we have successfully dismantled a large part of the threat.

Passenger Screening

One of our most important screening tools is information we collect about visitors seeking to enter the United States. We gather this information electronically through our Advance Passenger Information System (APIS), from Passenger Name Record (PNR) data, and through biometrics collection under US-VISIT.

Leveraging this information allows us to check passenger names against terrorist watch lists, search for connections between known and unknown terrorists, and run biometric finger scans against fingerprint databases and integrated watch lists in real-time. With these systems, we have prevented thousands of dangerous people from entering the United States, including individuals suspected of terrorism, murderers, rapists, drug smugglers, and human traffickers. Let me provide a couple of examples.

In May of this year, a British citizen attempted to board a flight from London to the United States. Using PNR data, U.S. Customs and Border Protection (CBP) officers determined the individual as a watch list match. Airline security officers prevented the man from boarding and he was turned over to British authorities for further questioning.

And in April of 2006, at Boston's Logan Airport, CBP officers used PNR information to identify two passengers whose travel patterns exhibited high-risk indicators. During the secondary interview process, one subject stated that he was traveling here on business for a group that is suspected of having financial ties to Al Qaeda. The examination of his baggage revealed images of armed men, one of them labeled "Mujahadin." Both passengers were refused admission.

This year we reached an important agreement with the European Union that will allow us to continue sharing PNR data while protecting passenger privacy. We will also continue to collect PNR data from flights originating in other regions around the world. In addition, we are moving forward with a regulation that will require general aviation aircraft entering the United States to provide comprehensive passenger manifest information to CBP prior to departure. This will help us prevent private aircraft from being used to bring potentially dangerous people or weapons into the United States.

In partnership with the Department of State, we are also expanding collection of biometrics at U.S. embassies and consulates overseas to include 10 fingerprints of an individual. The Department of State will have capabilities to collect 10 prints at all visa issuing posts by the end of CY 2007. This November, we expect to deploy 10 fingerprint collection capabilities to an initial set of ten U.S. airports, and we expect to have capabilities to collect 10 prints at all U.S. ports of entry by the end of CY 2008. Capturing 10 fingerprints will allow us to search databases for latent terrorist fingerprints. The Coast Guard also has implemented a program to collect biometrics on individuals

intercepted in the Mona Passage near Puerto Rico, giving us greater insight into who is seeking to enter the United States illegally through our maritime domain.

Secure Identification

As part of our Western Hemisphere Travel Initiative (WHTI), we've taken steps to prevent terrorists from using fraudulent documents to enter our country. As of January 23, 2007, citizens of the United States, Canada, Mexico, and Bermuda seeking to enter or re-enter the United States from within the Western Hemisphere must present a valid passport or acceptable alternative document if arriving by air.

Beginning January 31, 2008, we will also end the acceptance of oral declarations alone at the border and require U.S. and Canadian citizens to present either a WHTI-compliant document or government-issued photo identification, such as a driver's license, and proof of citizenship, such as a birth certificate, to enter the United States at land and sea ports of entry. We also anticipate fully implementing WHTI in 2008, whereby travelers will need WHTI-compliant documents – a passport, a passport card, a NEXUS card, or other acceptable document as defined in the WHTI final rule – for land and sea border crossings. We will consider a number of factors in determining the date for full implementation including the availability of WHTI-compliant documents.

The 9/11 Commission noted that for terrorists, travel documents are like weapons. We intend to take those weapons off the table. By requiring secure documents to enter the United States, we will make it harder for people to use fraudulent credentials to cross our borders, and we will make it easier for our inspectors to separate real documents from fake, enhancing our security and ultimately speeding up processing.

We also continue to work with states to enhance the security of driver's licenses under the REAL ID Act. Drivers' licenses are the primary form of identification in our country. We must make sure these documents are not easily forged or misused, and that consistent security standards are in place for their production. We are also actively engaging several states, including Washington, Vermont, and Arizona, and we are in discussions with several others to develop a more secure, enhanced driver's license that will strengthen border security and facilitate entry into the United States.

Border Security

Of course, we remain committed to effective border security to prevent the illegal entry of people between our ports of entry. Despite the failure this year to pass comprehensive immigration reform, we are aggressively moving forward to bolster security at the border in a number of important areas.

We have increased the size of the Border Patrol from approximately 9,000 agents in January 2001 to almost 14,500 agents today. We have worked with Governors to deploy thousands of National Guard forces to support construction of new fencing and vehicle barriers, with a target of 370 miles of fencing and 300 miles of vehicle barriers by the end

of next year. We have installed high-tech cameras and sensors, and deployed unmanned aerial vehicles as part of SBInet. We have expanded CBP air and marine branches to increase our coverage of the border. We have established Border Enforcement Security Task Forces to work collaboratively with state and local partners to fight criminal activity in border cities. And we have developed an Intelligence Campaign Plan for Border Security to provide comprehensive intelligence support for our operations.

As a result of these efforts, we have seen significant decreases in apprehensions – down 21 percent overall along our southern border, and in some sectors down as much as 68 percent – reflecting decreased flow due to stepped-up security. While we will never be able to hermetically seal our border, our efforts have strengthened our ability to keep dangerous people out of the country and have made our nation safer.

PROTECTING AGAINST DANGEROUS CARGO

Threats, of course, come in many shapes and sizes, including dangerous cargo infiltrating the international supply chain. Our greatest concern with respect to a cargo-borne threat is a terrorist attempting to smuggle a weapon of mass destruction into our country through our sea ports, land border crossings, or maritime borders.

Overseas Inspection

Since 9/11, we've built a system of layered security to identify and intercept such cargo before it reaches our shores. We now require advance information – including comprehensive manifest information and shipping history – on all containers bound for the United States, and we inspect all cargo that we deem to be high-risk. Through our Container Security Initiative, we've also deployed U.S. inspectors to 52 foreign seaports covering more than 80 percent of container traffic to the United States.

Radiological and Nuclear Detection

As part of our Secure Freight Initiative, in conjunction with the Department of Energy and the Department of State, we are also placing radiation detection equipment, imaging machines, and optical character readers in an initial set of seven foreign ports. Three of these ports – Port Cortes (Honduras), Port Qasim (Pakistan), and Southampton (U.K.) – will scan 100 percent of the cargo coming to the U.S., fulfilling Section 231 of the SAFE Port Act requirements. Operation testing on a more limited capacity will take place in the four remaining locations. This testing will provide important information on how we can address the unique screening challenges associated with larger and more complex ports.
At home, we've installed more than 1,000 Radiation Portal Monitors at critical seaports and land ports of entry to detect radiation before containers are allowed to enter the domestic supply chain. By the end of this year, we will scan nearly 100 percent of cargo for radiation at our major seaports and we will scan nearly 100 percent of cargo at all ports of entry by the end of next year.

We remain concerned that a small vessel could be used to launch a *U.S.S. Cole*-style attack against our maritime infrastructure or to smuggle dangerous weapons, materials, or people into our country. To address this threat, we continue to work with small vessel owners and operators across the country to better understand risks associated with small boats and to identify ways to improve our detection and tracking capabilities.

We also recently launched an initiative to reduce vulnerabilities associated with small vessels operating in U.S. waters. Through our West Coast Maritime Preventive Radiological Nuclear Detection pilot program, we will work with local authorities, beginning in the State of Washington, to conduct vulnerability and risk assessments and field evaluations; provide technical guidance and expertise; and deploy radiation detection technology and equipment to key maritime pathways with a view toward enhancing radiological scanning of small vessels.

PROTECTING CRITICAL INFRASTRUCTURE

Whether our aim is protecting boats, bridges, or other critical infrastructure, we cannot do so effectively without strong partnerships with private sector owners and operators of our nation's critical infrastructure. Consistent with our risk-management philosophy, we want to protect the most critical assets from the most serious threats.

Sector Specific Plans

Earlier this year, we completed all 17 Sector Specific Plans of the National Infrastructure Protection Plan. These plans are our roadmap for working with the private sector to assess vulnerabilities in our nation's infrastructure, set priorities, measure our effectiveness, and ensure accountability.

This is the first time in our nation's history that the government and the private sector have come together on such a large scale – across our entire economy – to develop a joint plan to reduce risk and protect key assets and resources. It is a tremendous milestone for our Department, the private sector, and the American people

Aviation Security

As we know, our nation's transportation sector remains a target for terrorists. Since 9/11 we have continued to add additional layers of security to protect the traveling public while ensuring its freedom of movement.

Our commercial aviation system now benefits from multiple security measures, including hardened cockpit doors, Federal Air Marshals, Federal Flight Deck Officers, 43,000 Transportation Security Officers trained to detect explosives materials and devices at checkpoints, explosives detection canine teams, 100 percent passenger and baggage screening, and enhanced inspection of air cargo.

To stay ahead of evolving terrorist threats, the Transportation Security Administration (TSA) has implemented a program to train its workforce to focus on passenger behavior for signs of malicious intent. The Screening Passengers by Observation Techniques (SPOT) program builds on proven methods to identify potential threats based on a person's behavior, not physical characteristics. This program already has proven successful. In August of this year, a TSA Behavioral Detection Officer trained under the SPOT program identified an individual at a ticket counter carrying a loaded gun and more than 30 rounds of ammunition. The SPOT program also has netted drug carriers, illegal aliens, and terrorism suspects.

In August of this year, TSA also published a proposed rule to streamline watch list procedures for domestic air travelers under our Secure Flight program. We intend to transfer control of watch lists checks from the airlines to TSA. This will result in greater consistency in how these checks are conducted and will reduce hassle for misidentified travelers.

Improvised Explosive Devices

Homeland Security Presidential Directive 19 established a national policy to protect our country against the threat of domestic improvised explosive devices (IED). We have seen the damage and loss of life that IED attacks have caused in Iraq and Afghanistan, and earlier this summer terrorists used a vehicle-borne IED in the attack against the Glasgow Airport. We must continue taking steps to prevent the use of such weapons in our own country.

To address this threat, our Science and Technology Directorate (S&T) has established a counter-IED task force to leverage existing multi-agency research and investments to deter, predict, detect, defeat, and mitigate the impact of IED attacks.

Beginning in FY 2008, S&T plans to accelerate and bolster its research and development of counter-IED technologies and products. S&T also continues its important work to develop, test, and evaluate a range of technologies and systems to detect explosives threats to air cargo systems, airport checkpoints, passenger baggage, mass transit systems, and critical infrastructure such as bridges and tunnels.

In addition, the Attorney General has led a review of ongoing activities in order to report to the President ways in which we might improve our security against terrorist use of explosives in the United States. The President called for this effort in Homeland Security Presidential Directive 19, and the Department of Homeland Security has been a leading partner in executing the President's direction.

Chemical Security

To keep dangerous chemicals out of the hands of terrorists, we have initiated a risk-based chemical security program using the regulatory authority we were granted last year by Congress.

In April of this year, we issued an interim final rule that requires chemical companies to assess the risks posed by their facilities and the chemicals they house or produce, and to implement security countermeasures to meet federal chemical security standards.

Because we want to approach chemical security comprehensively, we've also taken steps to protect dangerous chemicals in transit. Through agreements with the rail industry, we will reduce the time that rail cars carrying toxic inhalation hazards (TIH) remain at a standstill in rail yards. Further, last year we proposed regulations to require a positive chain of custody and better tracking capabilities for rail cars transporting TIH and other high-risk hazardous materials. In addition, we worked closely with the Department of Transportation on its proposed regulations to require rail carriers transporting TIH and other high risk materials to select the safest and most secure routes. When finalized, these actions will significantly reduce the risk of an airborne chemical threat endangering our cities and major population centers.

Biological Security

Providing early-warning biosurveillance information on human and animal health, the food and water supply, and the environment is critical to preventing a biological attack against our homeland or mitigating its impact.

Through the National Biosurveillance Integration Center, we are building an integrated system for collecting, monitoring and evaluating biological threat information so that we can rapidly characterize biological threats, whether man-made or naturally occurring. The center, which we expect will be fully operational by the end of next fiscal year, will integrate information coming from federal partners to develop a real-time understanding of the new and evolving biological threats we face.

Our BioWatch program also has been in continuous operation since 2003 and is present in more than 30 of our nation's largest metropolitan areas to provide an early detection capability in the event that a biological agent is released into the air. We are working on the development of the next-generation BioWatch system that will be fully automated to provide faster detection and analysis capability.

We also continue to work with our federal partners, including the Department of Agriculture and the Department of Health and Human Services (HHS), as well as state, local and private sector partners, to establish a well-coordinated readiness and response architecture for food and agro-defense. In addition, we've conducted formal risk assessments of 28 biological agents and used the resulting information to inform the acquisition of medical countermeasures by HHS and to prioritize and inform other national investments in biodefense.

Cyber Security

We must work in partnership with the private sector to protect our nation's cyber systems and to reduce our vulnerability to attacks that have the potential to cause serious disruption and economic damage.

Part of our strategy involves helping federal agencies regulate traffic on their cyber and communications networks using our "Einstein" intrusion detection system. Through our U.S. Computer Emergency Readiness Team (U.S. CERT), we also work with the public and private sectors to identify potential cyber threats, share warning information, and coordinate incident response activities.

For example, during a recent denial of service attack against the Government of Estonia, U.S. CERT leveraged international partnerships to quickly raise awareness of the attack, share information, and mitigate its impact. U.S. CERT coordinated with federal, international, and private sector partners to identify more than 2,500 sources of attack from 21 North Atlantic Treaty Organization (NATO) countries. This information was shared with military, intelligence, law enforcement, and CERT personnel from NATO member nations.

Through our Science and Technology Directorate, we are also conducting research, testing, and standards development to fortify our nation's communications infrastructure, including our cyber networks.

SHARING INFORMATION AND INTELLIGENCE

Of course, the common thread that ties together and supports all of these efforts is effective information collection, analysis, and sharing. I've said before that information is our radar for 21st century threats. Reliable, real-time information and intelligence allows us to identify and characterize threats, target our security measures, and achieve unity of effort in our response.

The Department of Homeland Security is both a collector of intelligence and a consumer of intelligence. Two of our components – the Coast Guard and our Office of Information and Analysis – sit at the table with the Intelligence Community and work hand-in-hand with our partners at the DNI, FBI, and NCTC.

Our department is also a tremendous consumer of intelligence. Intelligence shapes how we respond to threats, it arms our frontline personnel with information they need to do their jobs, it impacts how we invest our resources, and it allows us to make risk-based decisions.

We are dedicated to being a full partner within the Information Sharing Environment (ISE), and in so doing we are equally committed to sharing timely, relevant information with federal, state, local, private sector, and international partners.

Office of Intelligence and Analysis

Under the leadership of our Chief Intelligence Officer, we've refashioned and made more robust our intelligence enterprise at DHS. Our Office of Intelligence and Analysis (I&A) has improved the quality of intelligence analysis across the Department, including a focused effort to train our professionals to recognize information with intelligence value. I&A also has more fully integrated intelligence collection across the Department's components; raised our visibility within the Intelligence Community; and improved transparency with Congress.

To counter the threat of radicalization and extremism in our homeland, I&A also has created a branch focused exclusively on this issue. This branch seeks to expand our understanding of the "how and why" radicalizing influences take root. Our Office for Civil Rights and Civil Liberties is part of this focused effort to better understand radicalization, improve our capacity to counter domestic radicalization, and engage Muslim Americans, Arab Americans, and other key communities.

We remain committed to implementing the Intelligence Reform and Terrorism Prevention Act of 2004 and the President's directives to improve information sharing across our Department while protecting civil liberties and privacy. To this end, in February we issued a *Policy for Internal Information Exchange and Sharing Memorandum* to all DHS components to make sure they have access to terrorism, law enforcement, and homeland security information within DHS that is relevant to their mission. We also constituted an Information Sharing Governance Board, chaired by Charlie Allen, our Chief Intelligence Officer, to oversee the implementation of this policy. Hugo Teufel, our Chief Privacy Officer, sits on this board to ensure privacy and civil rights laws and policies are followed and institutionalized.

State and Local Fusion Centers

Of course, we must continue to share timely, relevant, and useful intelligence and information with the full range of our homeland security partners. Our goal is two-way flow. We want to provide useful information to our state and local colleagues, and we seek to benefit from their direct links to their communities and their visibility into potential terrorist plots developing at the grassroots level.

A major driver of this collaboration is State and Local Fusion Centers (SLFC) that promote information sharing and exchange across at all levels of government. We are working closely with the Program Manager for the ISE and the other members of the Information Sharing Council to support national efforts to include state, local and regional fusion centers as a robust part of the ISE.

We see tremendous value in creating a national network of state and locally run information clearinghouses that provide a clear, effective channel for information exchange as well as accurate, timely, and actionable intelligence products and services in support of homeland security.

We are working with the Department of Justice to gather, aggregate, and review data collected to evaluate the level of capability of state and major urban area fusion centers across the nation. Once this assessment process has been completed, we will be in a better position to offer recommendations to SLFCs on staffing, services, and resources.

To date, we have deployed 17 DHS intelligence officers to SLFCs across the country and we plan to have officers in as many as 35 sites by the end of fiscal year 2008. We are also deploying our Homeland Security Data Network (HSDN) to fusion centers to foster information sharing and exchange up to the Secret level. Twenty fusion centers will have HSDN access by the end of this year and we will double that capacity by the end of next year. In addition, we are building an analytic training program – equivalent to what we have for our own intelligence officers – for state and local analysts who work in fusion centers, and we are in the process of developing privacy and civil rights training.

Closed Circuit Television

States and cities have taken the lead in developing information and intelligence fusion centers with important support from our Department, including more than $300 million in grant funding. But another important counter-terrorism tool we continue to support is the development and deployment of closed circuit television (CCTV) systems.

Multiple cities – including New York, Chicago, San Francisco, and Philadelphia – have invested in CCTV systems to improve monitoring of potential incidents, protect transportation systems and critical infrastructure, and enhance response and mitigation measures.

We believe these systems, when used transparently and in accordance with appropriate privacy laws, have enormous potential to boost eyes on the ground, identify anomalous or threatening behavior, and aid in terrorist and criminal investigations. Indeed, we need look no further than the use of CCTV cameras following the terrorist attacks last year in London to see their potential benefits. The perpetrators of the attacks were identified with the help of London's camera network, and the four individuals who attempted to explode bombs in the subway two weeks later were swiftly identified and brought to justice through use of CCTV cameras.

CCTV systems are a critical component of our layered approach to securing critical infrastructure, and we will continue to allow states and cities to fund these systems using DHS grants.

National Applications Office

Finally, it is important that we use the technological assets of the Intelligence Community to our greatest advantage. To this end, our Department has established the National Applications Office (NAO) to leverage the assets and capabilities of the Intelligence

Community for civil applications, homeland security, and law enforcement purposes, including disaster preparedness, emergency management, and border security.

Our goal is to work with intelligence agencies to improve access to appropriate intelligence products for domestic users at all levels of government. The NAO will not expand existing capabilities or change how these systems are used. This program will also be subject to robust oversight by privacy and civil liberties offices within our Department, the DNI, as well as the independent Privacy and Civil Liberties Oversight Board.

WORKING AS ONE TEAM

Our value as a Department rests in our network of assets and people, and our ability to leverage that network to achieve integration and work effectively with our federal, state, and local partners.

While it will take time for us to reach full maturity, there is no question we have made substantial progress to build shared critical capabilities, work as one team, and create a Department that is more than the sum of its parts.

Part of our success in thwarting terrorist plots has been a direct result of our ability to work together. During the plot against fuel pipelines at JFK airport, our Department worked closely with the FBI to assess the threat to airport infrastructure, inform the owner of the pipeline, and release joint DHS-FBI intelligence products. Our Intelligence and Analysis Office and the Transportation Security Administration both played critical roles in supporting the investigation and eventually disrupting the plot.

Representatives from Immigration and Customs Enforcement also worked with the FBI to take down the terrorist plot against our military personnel stationed at Fort Dix, New Jersey. Our Department also closely coordinated with the FBI, other national security agencies, and our international partners during the liquid explosives threat to commercial aviation just over a year ago. During this threat, TSA deployed Federal Air Marshals to the United Kingdom and other international destinations to expand its mission coverage. CBP also increased its enforcement efforts within U.S. airports, deploying special response teams, canine units, and explosive detection technology.

CONCLUSION

On September 11, 2001, no one would have predicted the passage of six years without another terrorist attack on U.S. soil. Some believe our country hasn't suffered another attack because we've been lucky. Others contend the terrorist threat has diminished and we are no longer in danger.

I disagree. Over the past six years, we have disrupted terrorist plots within our own country and we've turned away thousands of dangerous people at our borders. We've

also witnessed damaging terrorist attacks against some of our staunchest allies in the war on terror.

I believe the reason there have been no additional attacks against our homeland is because we've successfully raised our level of protection and we've succeeded in frustrating the aims of our enemies. That's not to say our efforts have been flawless or that our work is done. On the contrary, we must move forward aggressively to build on our success to keep pace with our enemies.

Our improvements to passenger and cargo screening, critical infrastructure protection, and intelligence fusion and sharing must continue. While no one can guarantee we will not face another terrorist attack in the next six years, if we allow ourselves to step back from this fight, if we allow our progress to halt, if we don't continue to build the necessary tools to stay ahead of terrorist threats, then we will most certainly suffer the consequences.

I'd like to thank this Committee for your ongoing support for our Department. We look forward to working with you and with our federal, state, local, and private sector partners as we continue to keep our nation safe and meet our responsibility to the American people.