Testimony of

Secretary Janet Napolitano

U.S. Department of Homeland Security

Before the

United States Senate

Committee on Homeland Security and Government Affairs

September 13, 2011

Introduction

Thank you, Chairman Lieberman, Senator Collins, and members of the Committee. I appreciate the opportunity to testify today on the Department of Homeland Security's efforts to keep our nation safe from evolving threats.

The United States has made significant progress in securing the nation from terrorism since the September 11, 2001 attacks. As we observe this tenth anniversary of 9/11, we honor the nearly 3,000 innocent victims, as well as their friends, colleagues, and families. We salute the many first responders and law enforcement officials who responded with such courage and conviction on that tragic day and in the days that followed.

We also recommit ourselves to the continued protection of our nation, our freedoms, and our way of life. The recent anniversary is also a time to consider the great progress we have made since then. America is a stronger and more secure nation today. We bounced back from the worst attack on our soil and made progress on every front to protect ourselves, using our experience to become more resilient, not only to terrorist attacks, but to threats and disasters of all kinds.

Following 9/11, the federal government, including many members on this committee, such as Senators Lieberman and Collins, moved quickly to develop a security framework to protect our country from large-scale attacks directed from abroad, while enhancing federal, state, and local capabilities to prepare for, respond to, and recover from attacks and disasters at home.

A key element of this new security framework included the creation of the Department of Homeland Security (DHS) in March, 2003, bringing together 22 separate agencies and offices into a single, Cabinet-level department. Created with the founding principle of protecting the American people from terrorist and other threats, DHS and its many partners across the federal government, public and private sectors, and communities throughout the country have strengthened the homeland security enterprise to better mitigate and defend against dynamic threats.

Additionally, within the federal government, many departments and agencies contribute to this homeland security mission. The nation's armed forces serve on the front lines of homeland security by degrading al-Qa'ida's capabilities to attack the United States and targets throughout the world. The Office of the Director of National Intelligence, the Central Intelligence Agency, and the entire Intelligence Community, of which DHS is a member, are producing better streams of intelligence than at any time in history.

The federal homeland security enterprise also includes the strong presence of the Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI), whose role in leading terrorism investigations has led to the arrest of more than two-dozen Americans on terrorism-related charges since 2009.

We have also worked to build and strengthen the homeland security enterprise far beyond DHS and the federal government. A key part of the enterprise includes working directly with law

enforcement, state and local leaders, community-based organizations, and private sector partners to counter violent extremism at its source, using many of the same techniques and strategies that have proven successful for decades in combating violent crime in American communities.

Today I would like to highlight some of the Department's most significant work to address specific recommendations from the 9/11 Commission Report in the following areas:

- Expanding Information Sharing
- Developing and Implementing Risk-based Transportation Security Strategies
- Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel
- Enhancing Screening for Explosives
- Strengthening Efforts to Detect and Report Chemical, Biological, Radiological and Nuclear Threats
- Protecting Cyber Networks and Critical Physical Infrastructure
- Bolstering the Security of U.S. Borders and Identification Documents
- Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

While challenges remain, DHS continues to focus on minimizing risks while maximizing the ability to respond and recover from attacks and disasters of all kinds. This is a challenge that the more than 240,000 men and women of DHS commit themselves to everyday, with the support of Congress, our many partners within and outside of government, and the American people.

A 9/11 Timeline and Security Enhancements

Perhaps the best way to illustrate the concrete progress made over the past ten years is to apply today's security architecture to what existed when the terrorist attacks of 9/11 occurred.

The 9/11 plot, like many terrorist plots, began overseas, which means our security layers must start there as well.

- Intelligence: Planning for 9/11 began several years before the actual attacks. Osama Bin Laden summoned operatives to Afghanistan to discuss using commercial aircraft as weapons. Since then, we have strengthened the depth and breadth of our intelligence enterprise to get the best information possible, wherever the operational planning may occur.

- Visa Security: All of the 9/11 hijackers applied for visas overseas. Today, the DHS Visa Security Program deploys trained special agents to high risk posts around the world to conduct targeted, in-depth reviews of visa applicants before they ever reach the United States. We have additional layers of security in place through Department of State (DOS) visa checks and pre-departure screening measures.

- International Information Sharing: The hijackers began preparing for the attack while living abroad. Today 18 countries have joined the United States in agreeing to share information about potential terrorists and criminals through a series of Preventing and Combating Serious Crime Agreements. This is in addition to the many international

Mutual Legal Assistance Treaties and other arrangements with our partners and others in the international community.

After 9/11, the federal government discovered that information existed about the hijackers well before and after they came to the United States but this information had not been coordinated, shared and analyzed. Since 9/11, the federal government, along with its state, local, and private sector partners, has made significant improvements to enhance information sharing and analysis.

- Targeting: The federal government, and DHS in particular, has become more effective at analyzing travel-related data to better understand and anticipate the travel patterns of known or suspected terrorists. This analysis has been essential in identifying, targeting, and interdicting known and suspected terrorists – and prompting additional screening – before these individuals travel to the United States.

- Fusion Centers: Today, 72 recognized fusion centers serve as focal points for the receipt, analysis, gathering, and sharing of threat-related information among the federal government and state, local, tribal, territorial and private sector partners. Today the Intelligence Community is able to identify the common threads that can tie a seemingly minor crime to the larger threat picture – an important step that helps us to identify individuals such as the hijackers, many of whom were apprehended by law enforcement for routine traffic violations prior to 9/11.

Once the 9/11 hijackers made it to the United States, they still required access to the aircraft.

- Flight School: Prior to 9/11, the hijackers enrolled in flight school and conducted cross-country surveillance flights. Today, the Transportation Security Administration (TSA) screens all foreign students seeking flight training against terrorist, criminal history and immigration databases.

- Passenger Screening: Ten years ago, the 9/11 hijackers were able to purchase tickets and board planes carrying weapons. Today, through the Secure Flight program, DHS prescreens 100 percent of the 14 million passengers flying weekly to, from, and within the United States against the government watch lists. This enables us to identify and prevent individuals on the No Fly List from boarding aircraft and recommend others for enhanced screening. Moreover, Transportation Security Officers at more than 450 airports screen all checked and carry-on baggage for explosives, weapons, and other threats using cutting-edge technologies.

- Behavior Detection: Even though some of the 9/11 hijackers were randomly selected for additional screening and aroused the suspicion of gate agents, they still made it onto the plane. TSA's Behavior Detection Officers today work to identify potentially high-risk passengers who exhibit behaviors that indicate they may be a threat to aviation security and refer them for additional screening. TSA also conducts screening of passengers at boarding gates based on intelligence to help our security officers focus appropriate resources on determining if an individual presents a higher risk. Behavior Detection

serves as an important additional layer to enhance security in the airport environment, and can easily be deployed to other modes of transportation.

The last line of defense against threats to aviation security is on the plane itself.

- Airplane Security: Today, all commercial aircraft have hardened cockpit doors and Federal Air Marshals are deployed across the aviation system based on risk. Additionally, the Federal Flight Deck Officer program allows qualified pilots to use firearms to defend the cockpit, and TSA runs a crewmember behavior recognition and response training program. Taken together, these efforts significantly enhance the safety and security of passengers on board.

- Emergency Communications: Limitations in communication and interoperability among air traffic control operators, military personnel and first responders hindered the response on 9/11. Our nation has since made significant investments in training and technical assistance to improve emergency communications capabilities.

All of these layers combined create a much stronger security architecture that did not exist on 9/11 and that has helped keep our nation, our transportation system, and the American people safe over the past ten years.

During this time, we have also worked hard to create a unified and integrated department, focusing on accountability, transparency and leadership development, to enhance mission performance. This effort includes an ambitious series of management integration reforms to ensure the Department has the proper management structures and acquisition strategies necessary to succeed, attract and retain top talent, and build a culture of efficiency.

Progress Addressing Key Recommendations of the 9/11 Commission

Expanding Information Sharing

Over the past several years, DHS has strengthened and evolved our homeland security enterprise to better mitigate and defend against dynamic threats. This approach is based on the simple premise that homeland security begins with hometown security. Through close partnerships with federal, state, tribal, and local governments, community-based organizations, and private sector partners, DHS works to ensure that resources and information are available to state and local law enforcement, giving those on the frontlines the tools they need to protect local communities.

As part of this approach, we have supported the creation of 72 state and local fusion centers across our country, where information about threats is gathered, analyzed, and shared among our partners. Fusion centers also support and regularly interact with FBI Joint Terrorism Task Forces, which coordinate resources and expertise from across the federal government to investigate terrorism cases.

Since 9/11, DHS and DOJ have worked to establish and strengthen the Nationwide Suspicious Activity Reporting Initiative, which for the first time trains law enforcement across our country

to recognize behaviors and indicators related to terrorism and crime, and standardizes how those observations are documented, analyzed, and shared.

To help counter the threat of violent extremism in our communities, DHS also has trained more than 46,000 front-line law enforcement professionals, and worked with hundreds of communities and local organizations, to implement community-oriented policing strategies that have proven successful in crime-reduction efforts in some of our biggest cities.

In addition, we have implemented a new National Terrorism Advisory System (NTAS), which provides timely, detailed information about terrorist threats and recommended security measures to the public, government agencies, first responders, transportation hubs, and the private sector. Under NTAS, DHS coordinates with other federal entities to issue detailed alerts to the public when the federal government receives information about a specific, credible terrorist threat to the United States.

We also have worked to engage the broadest set of partners possible in our security efforts, because the reality is that no government entity, by itself, can protect a nation of our size and diversity. To this end, we have continued to strengthen and expand the "If You See Something, Say Something™" campaign, a nationwide effort to increase public awareness and the reporting of suspicious activity to the authorities. This campaign began in New York City, with the Metropolitan Transportation Authority of the State of New York. We have since expanded it to transit systems, federal buildings, major sports and entertainment venues, and major U.S. retailers.

In collaboration with the "If You See Something, Say Something™" campaign, TSA is also providing, through its First Observer™ program, training for thousands of state and local law enforcement personnel and private sector employees on how best to observe, assess, and report suspicious behavior at transportation and critical infrastructure sites and facilities across the country.

We also have focused on building stronger relationships with our many partners, including federal agencies, tribal governments and law enforcement, the private sector, and our international partners.

DHS works closely with its partners across the federal government on various information sharing initiatives to support law enforcement operations and protect the country from terrorists and other threats. For example, DHS has provided hundreds of personnel to FBI JTTFs, including U.S. Immigration and Custom Enforcement (ICE) special agents, U.S. Secret Service (USSS) agents, Federal Air Marshals, U.S. Customs and Border Protection (CBP) officers, U.S. Citizenship and Immigration Services (USCIS) officers and representatives from the Federal Emergency Management Agency (FEMA) and the U.S. Coast Guard (USCG).

DHS also has expanded our work with tribal governments and law enforcement across the nation. In 2009, DHS designated tribal liaisons in every operational component to work directly with tribal communities, and in 2011, DHS announced a new DHS Tribal Consultation Policy

outlining the guiding principles under which all elements of the Department are to engage with sovereign tribal governments.

The private sector also remains an integral component of the homeland security enterprise, and through the Department's Private Sector Office, we have worked to improve coordination of private sector engagement across the Department, facilitating more effective and rapid communication with key organizations and bolstering regionally-focused information sharing efforts.

Developing and Implementing Risk-based Transportation Security Strategies

DHS focuses on risk-based, intelligence-driven security across all modes of transportation. This approach emphasizes pre-screening for passengers and cargo to expedite travel for individuals that law enforcement knows the most about, while focusing limited resources on those who pose the greatest threat to the nation's transportation networks.

We have made significant advances in risk-based security, including conducting baseline security assessments across aviation, maritime, and surface transportation sectors; historic global aviation standards; advanced passenger and cargo information; and enhanced information sharing with international and private sector partners.

For example, after the attempted terrorist attack against Northwest Airlines Flight #253 on December 25, 2009, DHS launched an unprecedented initiative to strengthen global aviation against threats posed by terrorists, working in multilateral and bilateral contexts with governments as well as industry. These efforts culminated at the International Civil Aviation Organization (ICAO) Triennial Assembly in October 2010, where nearly 190 countries of the Assembly adopted the Declaration on Aviation Security, which forges a historic new foundation for aviation security to better protect the entire global aviation system and make air travel safer and more secure than ever before.

In June 2010, TSA also provided to Congress the Transportation Sector Security Risk Assessment report, a nationwide risk assessment that examines the potential threats, vulnerabilities, and consequences of a terrorist attack involving the nation's transportation system, including the aviation and surface domains. This report has informed the development of risk mitigation strategies, security standards, countermeasures, and resource allocations.

Since 2006, TSA also has completed more than 190 Baseline Assessments for Security Enhancement for mass transit, which provides a comprehensive assessment of security programs in critical transit systems around the country. Additionally, the DHS Science and Technology Directorate (S&T) has conducted detailed vulnerability analyses for all U.S. underwater mass transit tunnels. Since 2006, DHS has awarded over $2 billion in Surface Transportation Security Grants to help protect the public and nation's critical transportation infrastructure against acts of terrorism and other large-scale events.

DHS is also focused on strengthening maritime transportation security through a risk- and technology-based approach by evaluating vulnerabilities and mitigating threats across all

potential pathways. To this end, the United States Coast Guard's mix of cutters, aircraft, and boats as well as their unique authorities enhance layered maritime security from inspections at foreign ports of departure to patrols at the critical ports within our homeland. These measures increase transparency of activity, reduce risk, and maximize the effectiveness of maritime security resources.

To support state and local efforts to strengthen maritime security, since fiscal year 2003, DHS has provided more than $2 billion in grants for the Port Security Grant Program (PSGP) – awarded based on risk – to protect critical port infrastructure from terrorism, enhance maritime domain awareness and risk management capabilities, and support the implementation of the Transportation Worker Identification Credential (TWIC).

Enhancing Global Supply Chain Security

Immediately following the thwarted terrorist plot to conceal and ship explosive devices on aircraft bound for the United States in October 2010, DHS also worked with industry to implement additional precautionary security measures for international inbound flights. Today, DHS continues to work with leaders from global shipping companies and groups such as the International Air Transport Association (IATA) on developing preventive measures, including terrorism awareness training for employees and vetting personnel with access to cargo.

DHS is also working with agencies throughout the Administration to develop a unified vision for global supply chain security across air, land, and sea modes of transportation. The implementation of this strategy will more comprehensively address risk than ever before.

In support of our supply chain security efforts, CBP continues to operate the Container Security Initiative (CSI) to ensure that U.S.-bound maritime containers that pose a potential risk are identified and inspected before they are placed on vessels destined for the U.S. CSI, which was first announced in January 2002, is currently operational in 58 foreign seaports in 32 countries.

In January 2010, CBP also began enforcement of the Importer Security Filing and Additional Carrier Requirements interim final rule – also known as the "10 + 2 rule" – increasing the scope and accuracy of information gathered on cargo shipments arriving by sea into the United States and bolstering our layered enforcement strategy to protect against terrorism and other crimes at U.S. ports of entry. Further, CBP manages the Free and Secure Trade (FAST), a commercial clearance program for known low-risk shipments entering the U.S. from Canada and Mexico. Initiated after 9/11, FAST allows expedited processing for commercial carriers who have completed background checks and fulfill certain eligibility requirements.

In addition, the USCG's International Port Security personnel also inspect ports to ensure compliance with anti-terrorism protection measures and the International Ship and Port Facility Code. The USCG's International Training Team also works with the Department of State to build the capacity and proficiency of a foreign nation's Coast Guard and Naval forces to increase global supply chain security.

Strengthening Airline Passenger Pre-screening and Targeting Terrorist Travel

Prior to 9/11, screening of passengers coming to the United States was limited to the Department of State visa process and the inspection of a person by an immigration officer at the port of entry. Provision of advance passenger information (API) by airlines was voluntary and often inconsistent.

Over the past eight years, DHS has significantly adapted and enhanced its ability to detect threats, building a layered, risk-based system that includes a full range of identification verification measures – from visa application checks and biometric identification to the receipt of advanced passenger information and the full implementation of Secure Flight, a program that enables DHS to prescreen 100 percent of passengers flying to, from, or within the United States against government watchlists. DHS has also increased enrollment in its trusted traveler programs—which expedite travel for members who pass rigorous, recurrent security checks— to over one million members.

With support from international partners and the aviation industry, DHS has implemented pre-departure programs for U.S. bound flights as well as enhanced security measures to strengthen the safety and security of all passengers. These new measures, which cover 100 percent of passengers traveling by air to the United States, utilize real-time, threat-based intelligence along with multiple layers of security, both seen and unseen, to more effectively mitigate evolving terrorist threats.

DHS has worked closely with the intelligence and law enforcement communities to develop new mechanisms that identify high-risk travelers prior to departure. The U.S. Government has reformed the criteria and nomination processes for the consolidated terrorist watchlist and enhanced its information sharing capabilities to comprehensively connect available pieces of intelligence. This allows us to better identify individuals who are known to be of security concern as well as those individuals that would otherwise remain unknown.

Today, four centers across the federal government provide information regarding potential terrorist travel: Terrorist Screening Center (TSC), National Counterterrorism Center (NCTC), the National Targeting Center, and the Human Smuggling and Trafficking Center, all of which work together, leveraging threat-related intelligence and travel-related data which is essential in identifying, targeting, and interdicting known and suspected terrorists as well as suspicious cargo prior to entering the United States or boarding a flight bound for the United States.

In addition, information that previously had been retained at entry points in the United States is now shared overseas earlier in the travel continuum so that suspect travelers do not board an airplane departing for the United States without, at a minimum, additional screening. In fiscal year 2010, DHS identified more than 1,500 passengers on watchlists who had booked international flights departing to the United States. These passengers were denied boarding, received enhanced security screening, or were removed from the watchlist after it was determined that they did not pose a threat.

Prior to 9/11, there also was no advance screening of passengers seeking admission under the Visa Waiver Program (VWP), which enables nationals of 36 designated countries to travel to the

United States as nonimmigrant visitors for stays of 90 days or less without obtaining a visa. In 2008, DHS implemented the Electronic System for Travel Authorization (ESTA) to screen prospective VWP travelers against several databases, including the terrorist watchlist; lost and stolen passports; visa revocations; previous VWP refusals; and public health records. Since January 2009, nationals from all 36 VWP countries, regardless of their port of embarkation, have been required to obtain an approved travel authorization via ESTA prior to boarding a carrier to travel by air or sea to the United States under the VWP.

DHS – in cooperation with Departments of State and Justice – also has made substantial progress in bringing VWP countries into compliance with the information sharing requirements of the 9/11 Act, which requires VWP countries to enter into an agreement with the United States to report, or make available to the United States, lost and stolen passport data so that it can be screened against INTERPOL's Stolen and Lost Travel Document database. This requirement has contributed to the overall decline of fraudulent VWP passport intercepts at the U.S. border, from 712 in Fiscal Year 2004 to 36 in Fiscal Year 2010.

In addition, VWP countries must enter into an agreement to share information regarding whether citizens and nationals of that country traveling to the United States represent a threat to the security or welfare of the United States or its citizens. The Preventing and Combating Serious Crime Agreement, mentioned previously, goes toward satisfying this statutory requirement.

Through the Visa Security Program (VSP), with Department of State concurrence, ICE deploys trained special agents overseas to high-risk visa activity posts in order to identify potential terrorist and criminal threats before they reach the United States. ICE special agents conduct targeted, in-depth reviews of individual visa applications and applicants prior to visa issuance, and make recommendations to consular officers regarding refusal or revocation of visas when warranted. The VSP is currently deployed to 19 posts in 15 countries.

Advanced Passenger Information, Passenger Name Records, and Risk-Based Security

To identify high-risk travelers and facilitate legitimate travel, DHS requires airlines flying to the United States from foreign countries to provide Advanced Passenger Information (API), which includes basic information such as name, date of birth, citizenship/nationality and passport number, and Passenger Name Records (PNR), which includes information that travelers provide to airlines when booking their flights, such as itinerary, address, and check-in information, up to 72 hours prior to departure. Since the creation of the Department, DHS has improved its ability to use this and other information to target and identify both known and unknown individuals that are either a threat to aviation or the United States, and to prevent them from either flying to or entering the United States.

During 2008 and 2009, PNR helped the United States identify individuals with potential ties to terrorism in more than 3,000 cases, and in Fiscal Year 2010, approximately one quarter of those individuals denied entry to the United States for having ties to terrorism were initially identified through the analysis of PNR.

DHS and the European Union (EU) are completing a new U.S.-EU PNR agreement that improves the privacy protection and security benefits of the 2007 U.S.-EU PNR Agreement currently in effect. The new PNR Agreement, which requires approval by the Council of the European Union and ratification by the European Parliament, will underscore the United States and the European Union's continuing commitment to combat terrorism and serious transnational crime, while respecting privacy.

As noted earlier, DHS also fully implemented Secure Flight in November 2010, fulfilling a key 9/11 Commission recommendation. Secure Flight uses the passenger's full name, date of birth, gender, and if applicable, redress number, to conduct watch list matching prior to issuing the passenger a boarding pass. In addition to facilitating secure travel for all passengers, this program helps prevent the misidentification of passengers who have names similar to individuals on terrorist watchlists. Prior to Secure Flight, airlines were responsible for checking passengers against the watchlists. Through Secure Flight, TSA now vets over 14 million passengers weekly. In addition, DHS currently has eight Immigration Advisory Program arrangements in six countries, which enable our CBP officers posted at foreign airports to use advanced targeting and passenger analysis information to identify high-risk travelers at foreign airports before they board U.S.-bound flights.

In order to facilitate legitimate travel and effectively deploy screening and security resources, CBP has increased enrollment in its Trusted Traveler programs from approximately 80,000 members in 2003 to over one million today. CBP currently manages three Trusted Traveler Programs for the passenger environment: NEXUS, the Secure Electronic Network for Travelers Rapid Inspection (SENTRI), and Global Entry, and now offers a single, online trusted traveler application for all modes of travel. These programs expedite travel into the United States for pre-approved, low-risk members who voluntarily apply, pay a fee, provide biometric identification, pass a rigorous background check, and undergo recurrent security checks.

Recognizing that security screening must be constantly updated to address evolving threats, the Administration continues to focus on the implementation of risk-based measures to strengthen aviation security while improving the passenger experience wherever possible. TSA is currently working on a variety of identity-based screening measures that would enable travelers to volunteer more information about themselves, prior to flying, in order to expedite physical screening. This is an ongoing, collaborative effort with law enforcement, airport authorities, the aviation industry, and the traveling public. As risk-based screening evolves, DHS and TSA will continue to incorporate random security steps as well as other measures, both seen and unseen, in order to maintain the safest and most efficient system for the traveling public.

Enhancing Screening for Explosives

Prior to 9/11, limited federal security requirements existed for cargo or baggage screening. Today all checked and carry-on baggage aboard aircraft is screened for explosives. Increased levels of frontline security personnel at the passenger checkpoints and new technologies have also significantly enhanced security. In March 2002, TSA's first cadre of federal screeners totaled 80 individuals; today more than 52,000 TSA personnel serve on the frontlines at over 450 U.S. airports.

Increased Security at Airport Checkpoints

Through the American Recovery and Reinvestment Act of 2009 and annual appropriations, TSA has accelerated the deployment of new technologies at airports, including Advanced Imaging Technology (AIT) to detect the next generation of threats. In 2008, TSA began deploying AIT units, which resulted in the detection of hundreds of prohibited, illegal or dangerous items at checkpoints nationwide. AIT safely screens passengers for metallic and nonmetallic threats, including weapons, explosives and other objects concealed under layers of clothing. AIT has been evaluated and determined to be safe for all passengers by the Food and Drug Administration, National Institute for Standards and Technology and Johns Hopkins University Applied Physics Laboratory.

TSA ensures passenger privacy through the anonymity of AIT images—a privacy filter is applied to blur facial images; all images examined by TSA at airports are permanently and immediately deleted upon viewing; AIT images are not stored, transmitted or printed; the officer viewing the image never sees the passenger; and the officer assisting the passenger cannot view the image. TSA has begun installing automated target recognition software on millimeter wave AIT units that automatically detects potential threats without the need for screeners to view the AIT image, instead using a generic outline of a person for all passengers—further enhancing the privacy protections in place for AIT screening. Going forward, all millimeter wave AIT units that TSA deploys will include this new software. Backscatter AIT units will also have similar software installations.

TSA utilizes a range of technology to detect explosives at checkpoints, including Explosive Trace Detection units to screen carry-on articles, checked baggage, and passengers for explosive residue; Advanced Technology X-Ray machines that scan carry-on baggage from multiple angles, providing the operator with a clear image regardless of the bag's orientation within the machine; Bottled Liquid Scanners capable of detecting explosives and flammable liquids; and Explosive Detection Systems that screen checked baggage for explosives and can quickly determine if a bag contains a potential threat.

Increased Regulation and Security for Air Cargo

Prior to 9/11, limited federal security requirements existed for cargo screening. Now, in accordance with a Congressional mandate, 100 percent of all cargo transported on passenger aircraft that depart U.S. airports is screened commensurate with screening of passenger checked baggage. This milestone has been accomplished largely through the Certified Cargo Screening Program, which permits entities throughout the air cargo supply chain that have undergone rigorous inspection and certification processes to screen cargo.

In December 2010, TSA implemented requirements for 100 percent screening of high-risk cargo on international flights bound for the United States. DHS is also currently evaluating formal industry comment to a proposal to finalize its timeline for implementing the 100 percent international inbound cargo screening requirement. As part of this effort, TSA will work with

industry to leverage and enhance ongoing programs such as TSA's National Cargo Security Program recognition process.

In January 2011, DHS also launched a partnership with the World Customs Organization (WCO) to enlist other nations, international bodies and the private sector in increasing the security of the global supply chain—outlining a series of new initiatives to make the system stronger, smarter and more resilient. The three main elements of this international effort to strengthen the security of the global supply chain include preventing terrorists from exploiting the global supply chain to plan and execute attacks; protecting the most critical elements of the supply chain system, such as transportation hubs and related critical infrastructure, from attacks and disruptions; and building the resilience of the global supply chain to ensure that if something does happen, the supply chain can recover quickly.

As part of the effort to strengthen the global supply chain, ICE, in coordination with WCO, launched Operation Global Shield in 2010, a multilateral law enforcement effort aimed at combating the illicit cross-border diversion and trafficking of precursor chemicals for making improvised explosive devices (IED) by monitoring their cross-border movements. In March 2011, WCO voted to make the newly-renamed Project Global Shield a permanent program.

TSA also deploys canine teams to screen air cargo at the nation's highest cargo volume airports and provides explosives detection capabilities in the aviation, mass transit, and maritime transportation sectors. The TSA National Explosive Detection Canine Team Program has grown from 200 teams in 2001 to 900 teams in 2011. TSA has also developed a Passenger Screening Canine training program to enhance a canine's ability to detect explosive materials in baggage as well as on passengers.

Strengthening Efforts to Detect and Report Biological, Radiological and Nuclear Threats

Countering nuclear, biological, and radiological threats requires a coordinated, whole-of government approach. The Domestic Nuclear Detection Office (DNDO)—formed in 2005 as part of DHS—works in partnership with agencies across federal, state and local government to prevent attacks from radiological or nuclear materials through detection activities and and to deter attacks through forensics programs.

Working with partners from across the Administration, including the Departments of Defense, State, Energy, and Justice, the Intelligence Community, and the Nuclear Regulatory Commission, DNDO helps integrate interagency efforts to develop nuclear detection capabilities, respond to detection alarms, conduct research and development, and coordinate the development of the global nuclear detection architecture (GNDA).

In December 2010, DNDO submitted to Congress the GNDA Strategic Plan, an interagency product designed to guide the nation's nuclear detection capacity and capability development over the next five years. DNDO develops nuclear detection capabilities and implements the domestic portion of the GNDA in coordination with federal, state, local, international, and private sector partners as well as the Department's operational components.

For example, DNDO has worked with CBP to deploy Radiation Portal Monitors and other radiation detection technologies to seaports, land border ports, and mail facilities around the world. When the Department was formed in 2003, these systems scanned only 68 percent of arriving trucks and passenger vehicles along the Northern border. No systems were deployed to the Southwest border, and only one was deployed to a seaport. Today, these systems scan 100 percent of all containerized cargo and personal vehicles arriving in the U.S. through land ports of entry, as well as over 99 percent of arriving sea containers.

Additionally, DHS has procured thousands of Personal Radiation Detectors, Radiological Isotope Identification devices, and backpack detectors for CBP, USCG, TSA, and state and local law enforcement across the country to scan cars, trucks, and other items and conveyances for the presence of radiological and nuclear materials. DNDO has also made radiological and nuclear detection training available to over 15,000 state and local officers and first responders.

In its fiscal year 2012 budget request, DHS proposed expanding the Securing the Cities (STC) initiative, designed to enhance the nation's ability to detect and prevent a radiological or nuclear attack in the highest risk cities and urban areas while continuing to support efforts in New York. Through STC, nearly 11,000 personnel in the New York City region have been trained in preventive radiological and nuclear detection operations, and nearly 6,000 pieces of radiological detection equipment have been deployed.

DHS is also responsible for advancing the nation's nuclear forensics capability which, in conjunction with law enforcement and intelligence information, supports the identification of individuals involved in planned or actual attacks using radiological or nuclear weapons or materials. In fiscal year 2008, DNDO launched the National Nuclear Forensics Expertise Development (NNFED) Program—a collaborative effort with DOE and DOD to address the critical human capital needs of the technical nuclear forensics community.

One of DHS's highest priorities is preventing terrorist groups and hostile nations from illegally obtaining U.S. military products and sensitive technology, including components of weapons of mass destruction. To this end, ICE established the National Export Enforcement Coordination Network to better coordinate export enforcement efforts among law enforcement agencies and with the intelligence community.

Through another initiative called Project Shield America, ICE conducts outreach to manufacturers and exporters of strategic commodities that are believed to be targeted for procurement by terrorist organizations and the countries that support them, as well as countries identified as weapons proliferators. In November 2010, President Obama issued an Executive Order authorizing the establishment of the Export Enforcement Coordination Center to coordinate and enhance export control enforcement efforts among federal law enforcement agencies, export licensing agencies, and the intelligence community. The center will begin operations in late 2011.

The DHS Office of Health Affairs (OHA) coordinates the department's biological and chemical defense activities, providing medical and scientific expertise to support preparedness and response efforts. DHS S&T's Chemical and Biological Defense Division also works to increase

the nation's preparedness against chemical and biological threats through improved threat awareness, and development of advanced surveillance and detection, and responsive countermeasures.

Since the anthrax attacks 10 years ago, DHS also has made great strides in protecting the nation from, and preparing federal, state, and local governments to respond to biological attacks. In 2003, the Department stood up the BioWatch system—a federally-managed, locally-operated, nationwide environmental monitoring system designed to detect the intentional release of aerosolized biological agents which is currently operational in approximately 30 cities. In 2010, the Department began testing the next generation of automated early detection systems, known as Gen-3 which will reduce detection times.

To improve state and local biopreparedness, DHS established the first formalized sharing of public health and intelligence information with state and local health partners in 2009. In 2010, the Department developed and conducted a series of biological attack response exercises, including one in each of the 10 FEMA regions, involving more than 1,000 state and local officials. The Department has also contributed to the physical safety and security of biological select agent facilities by completing Buffer Zone Plans and Site Assistance Visits, and providing grant funding to first responders at these facilities.

Recognizing the critical need to dispense life-saving medical countermeasures to those potentially exposed to aerosolized anthrax spores within 48 hours of exposure, OHA started a program that ensures the Department's mission essential functions by distributing medical countermeasures to personnel serving in critical roles during an emergency.

Through the National Biodefense Analysis and Countermeasures Center (NBACC), S&T continues to provide critical biological threat analysis and forensic capabilities to understand the risks posed by biological threats and to attribute their use in bioterrorism or biocrime events. In addition, S&T supports the Chemical Security Analysis Center (CSAC) to increase awareness of chemical threats and the attribution of their use against the American public. S&T is also leading a joint effort known as the Integrated Consortium of Laboratory Networks (ICLN) to integrate and coordinate laboratory surge capacity in response to a significant chemical, biological, radiological attack or incident.

To save lives and expedite response efforts in the event of a terrorist chemical agent release inside a high-threat facility, DHS S&T also has developed the PROTECT system which is now deployed by jurisdictions through funding provided by the Transit Security Grant Program. PROTECT integrates detection, video surveillance, and operational communication systems for interior infrastructure protection for chemical incidents. In a demonstration, the system reduced the time responders appeared on scene from 30 minutes to 5 minutes

Protecting Cyber Networks and Critical Physical Infrastructure

Cybersecurity

Today's threats to cybersecurity require the engagement of the entire society – from government and law enforcement to the private sector and importantly, members of the public – to block malicious actors while bolstering defensive capabilities. DHS leads the whole of government effort to protect the federal executive branch civilian agencies and assisting the protection of the nation's critical infrastructure and critical information systems, where the government maintains essential functions and which provide services to the American people and support the financial services, energy, and defense industries.

In October 2010, DHS and DOD signed a Memorandum of Agreement to align and enhance America's capabilities to protect against threats to critical civilian and military computer systems and networks. The Agreement embeds DOD cyber analysts within DHS and sends a new team of DHS experts to NSA to be supported by DHS privacy, civil liberties, and legal offices.

In November 2010, the Multi-State Information Sharing and Analysis Center, opened the Cyber Security Operations Center, a 24-hour watch and warning facility, to enhance situational awareness at the state and local level and allow the federal government to quickly and efficiently provide critical cyber risk, vulnerability, and mitigation data to state and local governments.

In partnership with the private sector, the U.S. Computer Emergency Readiness Team (US-CERT) also takes proactive measures to stop possible threats from reaching an even broader audience by developing and sharing standardized prevention, mitigation, and response information products with its government and private sector partners. The DHS Office of Intelligence and Analysis also enables prevention, mitigation, and response through all-source intelligence analysis of cyber threats to federal Executive Branch civilian departments and agencies, state and local governments, and U.S. critical infrastructure and key resources.

Protecting critical infrastructure – including the systems and networks that support the financial services, energy, and defense industries – also requires a full range of partners, including other government agencies, the private sector and individuals. DHS led the development of the first-ever National Cyber Incident Response Plan to coordinate the response of multiple federal agencies, state and local governments, and the private sector to incidents at all levels.

In October 2009, DHS also opened the new National Cybersecurity and Communications Integration Center (NCCIC) —a 24-hour, DHS-led coordinated watch and warning center to serve as the nation's principal hub for organizing cyber response efforts and maintaining the national cyber and communications common operational picture.

DHS also utilizes the National Cybersecurity Protection System, of which the EINSTEIN intrusion detection system is a key component, to protect federal dot-gov domains. When fully deployed, the EINSTEIN system, initially deployed in 2004, will help block malicious actors from accessing federal executive branch civilian agencies, while working closely with those agencies to bolster their defensive capabilities.

Recently, DHS deployed EINSTEIN 2—a detection system that monitors federal internet traffic for malicious intrusions—at 15 Departments and agencies and four Managed Trusted Internet Protocol Service providers. At full operational capability, the next-generation EINSTEIN 3 will

provide DHS with the ability to detect malicious activity and disable attempted intrusions automatically, a significant improvement in the Department's ability to prevent cyber intrusions on federal executive branch civilian networks and systems.

Additionally, as part of the Comprehensive National Cybersecurity Initiative, DHS is working to reduce and consolidate the number of external connections that federal agencies have to the Internet through the Trusted Internet Connection (TIC) initiative. This initiative reduces the number of potential vulnerabilities to government networks and allows DHS to focus monitoring efforts and security capabilities on limited and known avenues for Internet traffic. In April 2011, the Obama Administration released the National Strategy for Trusted Identities in Cyberspace (NSTIC), which seeks to secure the identities of individuals, organizations, services and devices during select online transactions, as well as the infrastructure supporting the transaction.

To meet our future workforce needs, DHS is also building a world-class cybersecurity team by hiring a diverse group of cybersecurity professionals—computer engineers, scientists, and analysts—to secure the nation's digital assets and protect against cyber threats to CIKR. Through its Cybersecurity Workforce Initiative, DHS has increased its cyber staff by 500 percent while working with universities to build the cybersecurity pipeline through competitive scholarship, fellowship, and internship programs to continue to attract top talent. Additionally, DHS S&T co-sponsors national and regional cybersecurity competitions, at the high school and collegiate levels, to educate young individuals who can design secure systems and create sophisticated tools needed to prevent malicious acts.

Finally, DHS is committed to increasing public awareness about cybersecurity and empowering individuals and enterprises across cyber networks to enhance their own security operations. In 2010, the Department launched the *"Stop. Think. Connect."* public cybersecurity awareness campaign to increase public understanding of cyber threats and promote simple steps the public can take to increase their safety and security online.

Protecting Critical Infrastructure

Since fiscal year 2006, DHS has provided nearly $4 billion in grant funding through the Port Security, Transit Security and Buffer Zone Protection grant programs to protect critical infrastructure from terrorism. These grants support security plans, facility security upgrades, training, exercises, law enforcement anti-terrorism operations, and capital projects for risk mitigation of high threat infrastructure.

In 2009, DHS revised the National Infrastructure Protection Plan (NIPP) to integrate resilience and protection and broaden the focus of NIPP-related programs and activities to an all-hazards environment. DHS also developed an annual National Risk Profile that provides a multi-hazard assessment of risks facing critical infrastructure, including terrorist threats, cyber risks, and natural disasters.

Since 2007, DHS has implemented the Chemical Facility Anti-Terrorism Standards (CFATS) to regulate security at high-risk chemical facilities. To date, the Department has reviewed an estimated 40,000 consequence assessment questionnaires submitted by potentially high-risk

chemical facilities. Of these, approximately 4,500 facilities have been preliminarily identified as high-risk, resulting in the development and submission of Security Vulnerability Assessments. Of those facilities, most have received final high-risk determinations and have submitted or are in the process of completing Site Security Plans for DHS review to determine whether their security measures meet CFATS performance standards.

The Department's Office of Infrastructure Protection (IP) also has conducted more than 1,900 security surveys and more than 2,500 vulnerability assessments of the nation's critical infrastructure to identify security gaps and potential vulnerabilities and to provide protective measures recommendations to enhance the protection and resilience of the nation's critical infrastructure. In addition, IP has conducted more than 1,400 capability assessments of state and local bomb squads, explosives detection canine teams, dive teams, and SWAT teams to identify potential gaps and provide recommendations to mitigate vulnerabilities.

The Department also has deployed Protective Security Advisors (PSAs) to all 50 states, Puerto Rico, and the District of Columbia to support state, local, tribal and territorial officials and the private sector with critical infrastructure security efforts; coordinate and conduct vulnerability assessments and training; respond to all hazard incidents impacting critical infrastructure; and support effective information sharing and situational awareness. Additionally, the DHS S&T Directorate also conducts research and development to create new technologies to enhance critical infrastructure security.

Risk-based Security Grants

To support state, local, and tribal governments and the private sector in strengthening preparedness for acts of terrorism, major disasters, and other emergencies, since fiscal year 2003, DHS has awarded more than $32 billion in preparedness grant funding based on risk to build and sustain targeted capabilities to prevent, protect against, respond to, and recover from threats or acts of terrorism.

DHS continues to focus our grant funding on realizing and sustaining our operational priorities. For example, the fiscal year 2011 Urban Areas Security Initiative (UASI) grants encourage the development and sustainment of baseline capabilities at fusion centers. The UASI Program provides funding to address the unique planning, organization, equipment, training, and exercise needs of high-threat, high-density urban areas, and assists them in building an enhanced and sustainable capacity to prevent, protect against, respond to, and recover from acts of terrorism. Additionally, Transit Security Grant funding is prioritized based on risk and supports "shovel ready" security projects for critical assets.

Further, to address homegrown violent extremism, DHS has prioritized grant-funded prevention activities that directly support local homeland security efforts to understand, recognize, prepare for, prevent and respond to pre-operational activity and other crimes that are precursors or indicators of terrorist activity, while respecting privacy, civil rights and civil liberties protections.

Emergency Communications and Unified Incident Command

Since 9/11, DHS has worked to transform and strengthen interoperable communications across the country. Through the establishment of the Office of Emergency Communications, the awarding of more than $4 billion in dedicated grant funding for state and local interoperability efforts, and the development and deployment of new technologies, DHS has helped to enhance coordination to ensure that emergency response providers can communicate during natural disasters, acts of terrorism, and other catastrophic events. Additionally, in 2011, the Obama Administration announced a plan to deploy a nationwide, interoperable wireless broadband network for public safety.

DHS has made significant progress in establishing and improving a unified incident command system to respond to a wide range of threats, from natural disasters to coordinated attacks. The Incident Command System (ICS) provides a flexible mechanism for coordinated and collaborative management for many incidents, covering large or small geographical areas, single or multiple governments, nongovernmental, and/or private sector organizations. FEMA's disaster response operations are also organized along ICS principles. FEMA has established 25 Incident Management Assistance Teams (IMATs) that utilize the ICS as their core organizational management structure.

In 2010, DHS worked with 60 urban areas to assess emergency communications during a real-world situation. All 60 urban areas successfully demonstrated response-level emergency communications. These demonstrations illustrate how the significant organizational and technical investments funded through the Interoperable Emergency Communications and UASI Grants have improved their emergency communications capabilities in recent years.

DHS is also prioritizing private sector preparedness through programs such as the Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep™), Ready Business, the development and deployment of new technologies, and by incorporating private sector partners from the outset when developing new policies, programs and initiatives.

Bolstering the Security of U.S. Borders and Identification Documents

Protecting our nation's borders—land, air, and sea—from the illegal entry of people, weapons, drugs, and contraband is vital to the security and economic prosperity of our homeland. Over the past several years, DHS has deployed unprecedented levels of personnel, technology, and resources to the Southwest border. At the same time, DHS has made critical security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure while also strengthening efforts to increase the security of the nation's maritime borders.

Southwest Border

Over the past two years, the Obama Administration has deployed unprecedented levels of personnel, technology, and resources to the Southwest border. Today, the Border Patrol has more staff than at any time in its 87-year history. Along the Southwest border, DHS has increased the number of civilian boots on the ground from approximately 9,100 Border Patrol agents in 2001 to more than 17,900 today.

Under the Southwest Border Initiative, DHS has doubled the number of personnel assigned to ICE-led Border Enforcement Security Task Forces (BESTs), which work to dismantle criminal organizations along the border; increased the number of ICE intelligence analysts along the border focused on violence caused by transnational criminal organizations; tripled deployments of Border Liaison Officers to work with their Mexican counterparts; begun screening 100 percent of southbound rail shipments for illegal weapons, drugs, and cash; and expanded Unmanned Aircraft System (UAS) coverage to the entire Southwest border. There were no deployments of UASs along the Southwest border prior to 9/11.

Further, the $600 million supplemental funding requested by the Administration and passed by Congress in 2010 has enabled DHS to continue to add technology, personnel, and infrastructure to the Southwest border. These resources include 1,000 additional Border Patrol agents; 250 new CBP officers at U.S. ports of entry; 250 new ICE agents focused on transnational crime; improved tactical communications systems; two new forward operating bases to improve coordination of border security activities; and additional CBP UASs.

While this work is not yet complete, every key metric available shows that these border security efforts are producing significant results. Illegal immigration attempts, as measured by Border Patrol apprehensions, have decreased 36 percent in the past two years, and are less than one third of what they were at their peak. Seizures of drugs, weapons and currency have increased across the board. In fiscal years 2009, 2010, and the first half of 2011, CBP and ICE seized 75 percent more currency, 31 percent more drugs, and 64 percent more weapons along the Southwest border as compared to the same time period during the previous administration. Additionally, violent crime in U.S. border communities has remained flat or fallen in the past decade—in fact, studies and statistics have shown that some of the safest cities and communities in America are along the Southwest border.

In July 2011, the Obama Administration released its most recent National Southwest Border Counternarcotics Strategy, which provides the Administration’s overarching framework to address the threats posed by the illicit narcotics trade. DHS has also forged historic agreements with DOJ, increasing coordination between ICE and the Bureau of Alcohol, Tobacco, Firearms and Explosives and the Drug Enforcement Administration (DEA), on important Southwest border issues such as combating arms trafficking, bolstering information sharing and providing ICE agents the authority to work on important drug trafficking cases.

Further, President Obama authorized the temporary use of up to 1,200 additional National Guard personnel as a bridge to longer-term enhancements in border protection and law enforcement personnel from DHS to target illicit networks' trafficking in people, drugs, illegal weapons, money, and the violence associated with these illegal activities. That support has allowed DHS to bridge the gap and to hire the additional agents funded in the FY 2010 Border Security Supplemental to support efforts along the Southwest border.

In partnership with DEA and DOD, the Administration established the new Border Intelligence

Fusion Section within the El Paso Intelligence Center, which provides a comprehensive Southwest Border Common Intelligence picture, as well as real-time operational intelligence, to law enforcement partners in the region—further streamlining and enhancing operations.

The federal government has continued to work closely with state and local law enforcement along the border, serving together on task forces, conducting joint operations, providing the latest intelligence, and coordinating operational priorities.

Reflecting unprecedented collaboration, DHS and its Mexican counterpart agencies have signed numerous bilateral agreements and declarations to bolster and deepen collaboration and coordination in the areas of enforcement, planning, information sharing, and trade facilitation along the Southwest border. DHS works in partnership with DOS, DOJ and Mexico to implement Presidents Obama and Calderon's Declaration on 21st Century Border Management, pursuing initiatives and programs designed to expedite the legitimate flow of people and goods and focus law enforcement resources on those people and goods that represent the highest risk.

Northern Border

The Obama Administration has made significant advancements in creating a secure and resilient Northern border. DHS continues to invest in personnel, technology, and infrastructure, and to strengthen cooperation with federal, state/provincial, tribal, and private sector partners on both sides of the border. These achievements have resulted in a more secure Northern border that facilitates legitimate travel and trade.

DHS has made important security improvements along the Northern border, investing in additional Border Patrol agents, technology, and infrastructure. Currently, CBP has more than 2,200 Border Patrol agents on the Northern border, a 500 percent increase since 9/11. CBP also has nearly 3,700 CBP officers managing the flow of people and goods across ports of entry and crossings along the Northern border. In addition, CBP is using Recovery Act funds to modernize more than 35 land ports of entry along the Northern border to meet current security and operational needs.

The Department has also continued to deploy technology along the Northern border, including thermal camera systems, Mobile Surveillance Systems, and Remote Video Surveillance Systems, and successfully completed the first long-range CBP Predator-B unmanned aircraft patrol under expanded Federal Aviation Administration authorization that extends the range of approved airspace along the Northern border. Approximately 950 miles along the Northern border from Washington to Minnesota are currently covered by unmanned aircraft, in addition to approximately 200 miles along the northern border in New York and Lake Ontario—none of which were covered prior to the creation of DHS.

In February 2011, President Obama and Canadian Prime Minister Harper announced a landmark "Shared Vision for Perimeter Security and Economic Competitiveness" that sets forth how the two countries will manage shared homeland and economic security in the 21st century. This "Shared Vision" focuses on addressing threats at the earliest point possible; facilitating trade,

economic growth, and jobs; collaborating on integrated cross-border law enforcement; and partnering to secure and strengthen the resilience of critical infrastructure and cybersecurity.

As the lead agency for maritime border security, the USCG works with other federal, state, local and tribal partners to enhance security along the U.S. maritime border and uses interagency partnerships and international bilateral agreements to accomplish this mission. The USCG's overarching strategy is to improve maritime border security through a layered security system that begins beyond the country's physical borders. At-sea presence deters potential threats, provides mobile surveillance coverage, increases warning time, engages smugglers before they reach our shores, and enables USCG to address potential threats before they can cause harm to the United States.

Identification Documents and Biometrics

DHS has taken significant steps to strengthen security, reduce fraud and improve the reliability and accuracy of personal identification documents while enhancing privacy safeguards. This includes fundamentally transforming the way travelers enter the United States from within the Western Hemisphere through implementation of the Western Hemisphere Travel Initiative (WHTI) and from other countries around the world through the VWP, VSP and the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) program biometric identity and verification process.

In 2009, DHS implemented WHTI at land and sea ports of entry to strengthen border security for entry to the U.S., while facilitating legitimate travel and trade. WHTI requires that U.S., Mexican, Canadian and Bermudan citizens present a passport or other designated, secure travel document that denotes identity and citizenship when seeking to enter the United States. Prior to the implementation of WHTI, there was no documentary requirement for U.S. or most Canadian citizens to enter the United States from within the Western Hemisphere; travelers could present any one of numerous documents or simply make an oral declaration of citizenship. In 2005, DHS checked five percent of all passengers crossing land borders by vehicles against law enforcement databases. Today, due to WHTI, 97 percent of travelers are compliant with WHTI.

As noted earlier, DHS implemented ESTA in 2008 to screen VWP program applicants prior to travel to the United States and, as a result, has generally automated the arrival/departure form (Form I-94W) for authorized travelers arriving at airports or seaports from VWP countries. Through the Visa Security Program, which did not exist on 9/11, ICE, with Department of State concurrence, deploys trained special agents overseas to high-risk visa activity posts to identify potential terrorist and criminal threats before they reach the United States.

The US-VISIT biometric identity verification process collects digital fingerprints and a photograph from international travelers at U.S. visa-issuing posts and ports of entry to help Department of State officials determine whether a person is eligible to receive a visa and to assist CBP officers at ports of entry in determining whether a foreign national may enter the United States. This information is screened against the US-VISIT's IDENT database, a biographic and biometric repository, and is matched with biometric data collected previously from the person,

such as during a visa application, or a prior entry into the United States, to confirm whether the person is using his/her established identity.

To date, DHS has achieved ten-fingerprint identity verification for 99 percent of air and sea points of entry. Prior to 9/11, there was no capability to verify a visitor's claimed identity beyond a visual check of their identification documents.

DHS is also undertaking a Department-wide effort to address the backlog of unvetted potential visa overstays, an issue identified by the U.S. Government Accountability Office (GAO) in its April, 2011 report. The goal of this ongoing effort is not only to identify which individuals have overstayed their visas, but also to prioritize for removal identified overstays who may be a threat to national security.

In addition, USCIS continues to enhance fraud detection and national security capabilities to ensure that immigration benefits are not granted to individuals who pose a threat to national security. USCIS has embedded Fraud Detection and National Security officers in eight other government agencies to increase information sharing and collaboration efforts that enhance law enforcement and intelligence operations. Further, USCIS has implemented a new state-of-the-art system that enhances the verification and sharing of electronic records and has redesigned all of its secure identity documents to comport with the latest DHS and International Civil Aviation Organization standards as well as best practices in industry and government.

Since 2009, USCIS has incorporated the use of electronic fingerprints in all of its overseas programs to enhance the accuracy and effectiveness of its verification checks. The new Permanent Resident Card (commonly referred to as a "green card"), implemented in 2010, includes new security features that reduce the risks of counterfeiting, tampering, and fraud; it also includes a radio frequency identification tag that serves as a pointer to a record in a secure DHS database. USCIS has also updated the Employment Authorization Document, known as "work permit," by adding a machine-readable zone.

Since 2007, DHS also has enrolled over 1.9 million port workers and merchant mariners in the Transportation Worker Identification Credential (TWIC) program, and issued a tamper-resistant biometric credential to those who require unescorted access to secure areas of ports and vessels and who were determined not to present a security risk.

Additionally within the maritime domain, the USCG has implemented a mobile biometrics collection system to identify undocumented migrants and match them against known databases of past criminal and immigration violations as well as terrorist watchlists, enabling the USCG to prosecute repeat offenders. Through June 2011, the USCG has identified more than 900 individuals who were enrolled in US-VISIT's IDENT biometric database as prior felons, violators of U.S. immigration laws, or other persons of interest and referred them to law enforcement authorities for appropriate action.

Ensuring Robust Privacy and Civil Rights and Civil Liberties Safeguards

DHS has the first statutorily required privacy office of any federal agency, and the Department builds privacy and civil rights and civil liberties protections into its operations, policies, programs, and technology deployments from the outset of their development.

The DHS Privacy Office partners with every DHS component to assess policies, programs, systems, technologies, and rulemakings for privacy risks, and recommends privacy protections and methods for handling personally identifiable information.

DHS's Office for Civil Rights and Civil Liberties (CRCL) plays a key role in the Department's mission to secure the nation while preserving individual freedoms and represents the Department's commitment to the idea that core civil rights values – liberty, fairness, and equality under the law – are a vital part of America, and that these values provide a bulwark against those who threaten our safety and security. Since its inception, CRCL has expanded its participation in programs and activities throughout the Department and continued its efforts to promote civil rights and civil liberties.

CRCL's community engagement efforts include a wide variety of stakeholders and organizations through regular roundtables across the country. CRCL has also expanded its training capacity and worked closely with the DHS Privacy Office and the Office of Intelligence and Analysis to offer civil rights and civil liberties training for fusion centers, as well as training to a number of the Department's federal, state, and local partners.

Challenges that Remain

While DHS has made great progress in securing the nation since the September 11, 2001 attacks, challenges remain in implementing key recommendations in the 9/11 Commission Report.

Despite significant efforts, including the proposed PASS ID legislation to enhance the security of driver's licenses, many states are still unable to fulfill the congressionally mandated REAL ID requirements. The Department also continues to undertake new steps to increase the use of risk based security screening; develop strategies to guard against an increasing volume of cyber attacks; partner with first responders to address interoperability challenges; and determine a cost-effective means to implement a biometric exit solution.

While the demands on DHS have never been greater, the current fiscal climate requires the Department to continue to maximize every security dollar. In order to preserve front line security operations, DHS has identified over $1 billion in cost avoidances and cuts under this Administration. In addition, the Department's fiscal year 2012 budget request included more than $800 million in further reductions associated with administrative savings and efficiency initiatives currently underway, from efforts to reform acquisition, asset and real property management to cuts to professional services contracts, supplies and materials, printing, and travel.

Additionally, it is my hope that Congress will address an unmet 9/11 Commission recommendation that is solely within its power to solve. Effective congressional oversight is critical to promoting transparency, accountability and efficiency. The 9/11 Commission Report

recognized that the existing structure of fragmented and disparate oversight over DHS requires significant department resources and hinders Congress's ability to provide the department with clear oversight and guidance. We can all agree that reforming this system will be good for Congress, DHS and the American people.

Conclusion

While America is stronger and more resilient as a result of these efforts to strengthen the homeland security enterprise, threats from terrorism persist and continue to evolve. Today's threats do not come from any one individual or group. They may originate in distant lands or local neighborhoods. They may be as simple as a homemade bomb or as sophisticated as a biological threat or coordinated cyber attack.

Increasingly, state, local, and tribal law enforcement officers, as well as citizens, businesses, and communities are on the frontlines of detection and prevention. Protecting the nation is a shared responsibility and everyone can contribute by staying informed and aware of the threats the country faces. Homeland security starts with hometown security—and we all have a role to play.

I want to thank Congress – and this Committee in particular – for your role in the creation of the Department, your continued support for our critical efforts, and your invaluable guidance and oversight as we continue to work to create a stronger and safer country.

I have stated before that we cannot put our country under a glass dome or guarantee we will never again face another terrorist attack. But we will do everything within our power to secure our nation against a large attack or disaster, to protect critical infrastructure and cyber networks, and to continue to engage a broader range of Americans in our shared responsibility for security. I look forward to any questions you may have.