Testimony of

The Honorable Asa Hutchinson

Undersecretary for Border and Transportation Security Directorate
Department of Homeland Security
August 19, 2004

BEFORE THE SENATE JUDICIARY COMMITTEE
August 19, 2004

Chairman Hatch, Ranking Member Leahy, and other distinguished members. It is a pleasure to appear before you today to discuss how the Department of Homeland Security (DHS) is addressing the recommendations from the September 11 Commission Report relating to law enforcement, border security, and the USA PATRIOT Act.

As this Committee and the American people know, since the terrible events of September 11th, our federal law enforcement agencies have been heavily focused on ferreting out terrorists and their supporters. The DHS law enforcement agencies, and its predecessors, have been relentlessly pursuing the terrorists and their financial trails while protecting the privacy interests and civil liberties of our citizens.

At DHS, we are actively sharing information with all relevant federal and state law enforcement agencies, State, territorial, tribal, and local officials, and the private sector, using information we learn every day to refine our analytical tools we use to help identify terrorists and their supporters before they can reach America's shores, and employing new and emerging technologies, such as biometrics, in innovative ways to secure America and to preserve its economic security.

The American people can be proud of our efforts and achievements. I am honored to lead, under the direction of Secretary Ridge, the largest law enforcement component of DHS and represent them here today.

The Challenge

The challenge that DHS faces is enormous. We share nearly 7,500 miles of land border with Canada and Mexico, across which more than 326 million people, 119 million motor vehicles, 11 million truck containers, and 2.5 million rail cars pass every year. We patrol almost 95,000 miles of shoreline and navigable waters, and 361 ports that see over 203,000 vessels, 9 million containers of cargo, and nearly 15 million cruise and ferry passengers every year.

We have some 445 primary airports and another 124 commercial service airports that see 30,000 flights and 1.8 million passengers every day. There are approximately 110,000 miles of highway and 220,000 miles of rail track that cut across our nation, and 590,000 bridges dotting America's biggest cities and smallest towns.

Every day, our job is to work to make our country more secure. We are constantly evaluating our intelligence and a threat environment that literally changes by the hour and day.

Even in this ever-changing environment, however, we believe that terrorists will consistently target certain sectors and consistently look to use certain types of attack. That knowledge allows us to operate at a high level of awareness.

9/11 Commission Recommendations

Let me address the recommendations of the 9/11 Commission that are most relevant to this Committee and this hearing.

Targeting Terrorist Financing

The 9/11 Commission noted that, "[v]igorous efforts to track terrorist financing must remain front and center in U.S. counterterrorism efforts. The government has recognized that information about terrorist money helps us to understand their networks, search them out, and disrupt their operations."

DHS fully agrees.

Since the day DHS came into existence, we have continued the exemplary work of the former U.S. Customs Service to investigate terrorist financing schemes.

Unprecedented Interagency Cooperation

We have worked in close cooperation with the FBI on these cases. In an unprecedented exchange of information sharing between federal law enforcement agencies, our Bureau of Immigration and Customs Enforcement (ICE) vets all of its terrorist financing leads through the FBI pursuant to a Memorandum of Agreement (MOA) between DOJ and DHS.

ICE and the FBI have established a Joint Vetting Unit staffed by senior personnel from each agency to identify investigations with a potential nexus to terrorist financing. ICE has also detailed a senior-level manager to the FBI's Terrorist Financing Operations Center (TFOS) as the Deputy Section Chief. Thus, the FBI and DOJ are immediately aware of all ICE cases that relate to terrorist financing.

When an ICE investigation has a nexus to terrorism or terrorist financing, the investigating ICE field office is instructed to contact the appropriate FBI field office to arrange for a smooth transition of the investigation to the Joint Terrorism Task Force (JTTF).

ICE has also entered discussions with the Drug Enforcement Administration (DEA) about sharing information related to the counter-narcotics enforcement mission of each agency. DHS is seeking reciprocal access to FBI and DEA databases in order to strengthen the ability of DHS to perform its various missions more effectively and efficiently.

DHS and ICE have taken the fight against terrorist financing to the next level. The same weaknesses and vulnerabilities that organized criminal groups exploit today in our border security can be used tomorrow by terrorists and their supporters. Organized criminal groups who today smuggle narcotics or other commodities, like cigarettes or counterfeit merchandise, can tomorrow smuggle potential weapons of mass destruction using their existing networks. Similarly, groups who today specialize in smuggling undocumented aliens into the country can be used tomorrow to aid terrorists in evading inspection at the border.

Cornerstone

In response, ICE initiated the Cornerstone program to focus on the systems that criminals, including terrorist groups, alien smugglers, and Intellectual Property Rights (IPR) violators use to earn, store, and move their proceeds. Cornerstone is designed to identify potential vulnerabilities in our trade and financial systems that can compromise our economic security.

Through Cornerstone, ICE agents build partnerships and exchange information with the private businesses and industries that terrorists and other criminal organizations seek to use and exploit. This partnership enables ICE to provide timely information and feedback to the private sector so that they can take the appropriate precautions to protect themselves. ICE also receives information, tips, and insights from the businesses and industries that are the first to encounter and recognize possible indications of terrorist activity.

As part of Cornerstone and protecting the economic security of our homeland, ICE investigates money laundering related to banks and other traditional and non-traditional financial institutions, trade-based money laundering, the smuggling of bulk currency, the illegal use of money remitters and money service businesses, commercial fraud, IPR violations, cybercrime, and the illegal trade in weapons and dual-use goods and technology.

Targeting Terrorist Travel

The 9/11 Commission also stated that, "[t]argeting travel is at least as powerful a weapon against terrorists as targeting their money. The United States should combine terrorist travel intelligence, operations, and law enforcement in a strategy to intercept terrorists, find terrorist travel facilitators, and constrain terrorist mobility."

We have implemented a number of successful programs to deny terrorists the ability to travel freely into the U.S., identify potential travel facilitators, and constrain the mobility of known and suspected terrorists.

The two I would like to focus on today are our creation and use of the National Targeting Center and our US-VISIT biometric screening system.

National Targeting Center

The NTC began around-the-clock operations on November 10, 2001, providing tactical targeting and analytical research support for the anti-terrorism efforts of the former-U.S Customs Service. The NTC is primarily staffed by DHS's Bureau of Customs and Border Protection (CBP). The NTC staff consists of CBP officers and field analysis specialists who are experts in passenger and cargo targeting for air, sea, and land operations in the inbound and outbound environments. The

NTC develops tactical targets - potentially high-risk people and shipments that should be subject to a CBP inspection - and it develops these targets from raw intelligence, trade, travel, and law enforcement data.

NTC supports DHS field elements, here and overseas, including Container Security Initiative (CSI) personnel stationed in 21 countries throughout the world, the Visa Security Program, the Immigration Security Initiative , currently operated out of Schiphol Airport in Amsterdam, and to CBP Officers at all of our ports of entry, as well as between the ports through support to CBP's Office of Border Patrol.

During the period of heightened alert last December, the NTC played a pivotal role in analyzing passenger manifest information related to several international flights that were determined to be at risk, in order to ensure that passengers on board did not pose risks to the flights.

The NTC includes representatives from ICE, the FBI, the intelligence community, the Transportation Security Administration (TSA), US-VISIT, the Department of Energy, the Department of Agriculture, the Food and Drug Administration, and the United States Coast Guard.

The NTC uses the Automated Targeting System (ATS) to identify and target high-risk passengers and cargo entering the United States. ATS permits the NTC's trained personnel to process advance passenger information, to recognize anomalies and "red flags" and to determine which individuals and shipments should be given greater scrutiny at our ports of entry.

CBP continues to work on a version of ATS that, for the first time, will be able to identify potentially high-risk travelers in passenger vehicles. The new version of ATS will also increase the amount of government data that the system can access and analyze and enable us to train more people on the use of the system.

These, and many other U.S. intelligence analysis capabilities, are being used to help exploit terrorists' vulnerabilities as they travel and to learn more about their activities and methods. In addition to our ongoing efforts to target terrorist travel to, from, and within the United States, the Administration is seeking, on both a bilateral and multilateral basis, to promote similar efforts by other responsible governments, and to provide those governments with relevant terrorist-related information.

US-VISIT

Prior to the terrorist attack on September 11, Congress twice mandated the creation of an electronic entry-exit system. Following the events of September 11, Congress added the requirement that the entry-exit system incorporate biometric technology as a means to verify the identity of foreign travelers. DHS established the US-VISIT program ahead of schedule, and began operating US-VISIT at 115 ports of entry on January 5, 2004.

US-VISIT enhances the security of our citizens and visitors; facilitates legitimate travel and trade; ensures the integrity of our immigration system; and protects the identities and privacy interests of our visitors.

In addition to developing an integrated system that records the arrivals and departures of travelers and uses biometric technology to combat fraud, DHS designed US-VISIT to: (1) provide information to CBP Officers and consular officers for decision making purposes; (2) reflect any pending or completed immigration applications or actions; (3) identify nonimmigrant overstays; and (4) provide accurate and timely data to appropriate enforcement authorities. US-VISIT accomplishes all these objectives.

US-VISIT represents a major milestone in enhancing our nation's security and our efforts to reform our borders. It is a significant step towards bringing integrity back to our immigration and border enforcement systems. It is also leading the way for incorporating biometrics into international travel security systems.

Integrated Entry-Exit System

US-VISIT is a continuum of security measures that begins before individuals enter the United States and continues through their arrival and departure from the country. Enrolling travelers in US-VISIT using biometric identifiers allows DHS to:

? Conduct appropriate security checks: We conduct checks of visitors against appropriate lookout databases and selected criminal data available to consular officers and CBP Officers at the ports of entry, including biometric-based checks, to identify criminals, security threats, and immigration violators.
? Freeze identity of traveler: We biometrically enroll visitors in US-VISIT - freezing the identity of the traveler and tying that identity to the travel document presented.
? Match traveler identity and document: We biometrically match that identity and document, enabling the CBP Officer at the port of entry to determine whether the traveler complied with the terms of her/his previous admission and is using the same identity.
? Determine overstays: We will use collected information to determine whether individuals have overstayed the terms of their admission. This information will be used to determine whether an individual should be apprehended or whether the individual should be allowed to enter the U.S. upon her/his next visit.

The DHS and Department of State (DOS) together have created a continuum of identity verification measures that begins overseas, when a traveler applies for a visa, and continues upon entry and exit from this country. The system stores biometric and biographic data in a secure, centralized database and uses travel and identity documents to access that information for identity verification and watchlist checks. Today, more than 180 nonimmigrant visa-issuing posts and 90 immigrant visa issuing posts capture fingerscans and digital photographs of foreign nationals when they apply for visas, regardless of their country of origin. This process will be in place at all 211 visa-issuing posts worldwide within 60 days. In addition, on September 30, 2004, nationals from Visa Waiver Program (VWP) countries will be enrolled in US-VISIT when they travel to the United States.

At assigned U.S. border points of entry, designated visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against various databases, which US-VISIT has successfully integrated and which contain visa issuance information, terrorist and criminal watchlists, and immigration status information. That information allows a CBP Officer at the border to verify the identity of the traveler and to determine whether the foreign national is a public threat or is otherwise inadmissible. In its first 7 months of operation, DHS processed nearly 7.3 million foreign national applicants for admission through US-VISIT at its air and sea ports of entry. During that period, 674 individuals were identified by biometrics alone as being the subject of a watchlist lookout.

Our experience with biometrics is demonstrating that our ability to identify who entered and left the country is significantly improved with the addition of biometric identifiers. Here are some examples of US-VISIT intercepts:

? At Newark international airport, an international traveler appeared for inspection. Standard biographic record checks using a name and date of birth cleared the system without incident. However, a scan of the traveler's index fingers, checked against the US-VISIT biometric database, revealed that the traveler was using an alias and was, in fact, a convicted rapist. Additionally, he had previously been deported from the United States. US-VISIT's search disclosed that the individual used at least nine different aliases and four dates of birth. He had previously been convicted of criminal possession of a weapon, assault, making terrorist threats, and rape.
? CBP Officers at JFK International Airport processing a passenger through the US-VISIT procedures found that the individual was using an alias. Further information uncovered two arrests for aggravated trafficking of drugs, a subsequent failure to appear, and visa fraud. The traveler had used this fraudulent visa to enter the United States over 60 times without being detected by standard biographic record checks, the last time only 11 days earlier.
? Recently, a traveler with four aliases, three social security numbers, and a criminal history going back to 1990, tried to enter the United States. He was not admitted because a comparison of his fingerscans against the US-VISIT biometric watch list determined that he had previously been deported from the United States.

As these examples demonstrate, US-VISIT works.

Monitoring the status of visitors while in the United States is an integral part of border management and ensures the integrity of the immigration system. One of the US-VISIT Program's primary roles in status management is identifying those individuals who have overstayed the terms of their admission - calculated through the exchange of information from appropriate case management systems, especially those managed by U.S. Citizenship and Immigration Services (CIS). Incorporating biometrics into US-VISIT allows us to positively identify individuals who have overstayed their admission and gives DHS the ability to identify immigration benefits and visa fraud by identifying individuals who try to misrepresent their status or their identity.

Currently, our exit procedures are based largely upon biographic departure information from carrier produced passenger manifests. We match this information with the admission information and identify those likely to have overstayed the terms of their admission. Our goal is to enhance our ability to match arrivals and departures by using biometrics. We are testing this with various pilot programs at Baltimore-Washington International Airport, the Miami Cruise Terminal, and Chicago O'Hare Airport. We plan to expand our pilot program to a total of 15 air and seaports over the next several months. Through the pilot programs, we will test different options and evaluate the results to identify the most effective, cost-efficient process.

US-VISIT is achieving success because of biometric technology - matching digital fingerscans against lookout, criminal history, and enrollment data makes US-VISIT more effective.

Deterring the Use of Fraudulent Documents

The Commission's report noted that terrorists use altered and counterfeit travel documents to evade detection. In the border and immigration enforcement arenas, biometric identifiers are tools that help prevent the use of fraudulent identities and travel documents. The purpose of the biometric identifier is to verify a person's identity in order to run criminal history checks and to ensure that an individual cannot apply and/or be granted benefits under different names. Biometric visas issued by the DOS to travelers to the United States allow one-to-one matches, to verify that the person presenting the visa is the person who was issued the visa, and one-to-many matches, to ensure that the bearer is not the subject of a biometric lookout or enrolled in the system under another name. Like the biometric visa process, US-VISIT enrollment fixes a person's identity. When a VWP traveler enrolls in US-VISIT, the person's fingerprints will be electronically linked to the passport, thus preventing another person from using that passport by freezing identities at the border and ensuring that the person is not enrolled under another name.

Sharing US-VISIT Data

The information integrated by US-VISIT includes appropriate biographic, biometric (i.e. fingerscans and digital photographs), and other immigration-related information. This information is collected or verified at each contact with the individual. Sharing the information in a timely manner with appropriate decision makers, ensures that they can make the best decisions possible. These decision makers include consular officials from the Department of State; and Customs and Border Protection officers, Immigration and Customs Enforcement agents, and U.S. Citizenship and Immigration Services officers from the Department of Homeland Security and other appropriate law enforcement officials. The vast majority of individuals whose information we collect are legitimate travelers who comply with U.S. laws. US-VISIT has established a data-sharing environment that specifies the security, privacy-related, and retention requirements that must be implemented by entities using US-VISIT information on a routine basis to protect the information provided by these individuals.

Safeguarding the Personal Privacy of Our Visitors.

An obvious concern for all legitimate travelers is that criminals will use their lost or stolen travel documents to enter the United States. Biometric identifiers make it difficult for criminals to travel on someone else's travel documents. This is a significant benefit that US-VISIT delivers for the millions of legitimate travelers the U.S. welcomes each year.

We must continue to respect the privacy of our visitors. Because the data we now collect from foreign nationals is considered to be highly personal and potentially subject to abuse, DHS has taken the extraordinary step of applying aspects of the U.S. Privacy Act of 1974 to this group of foreign nationals. Our approach has garnered widespread praise from privacy advocates and the general population of foreign travelers coming to the United States as well as some of our closest allies. These stakeholders have made it clear in the press, and in comments sent to us, that they expect us to honor our commitment to take the necessary steps to only use the information for the purposes stated.

Although biometric identifiers in the form of photographs and fingerprints have long played a key role in securing our borders, manually matching this information is subject to high costs and slow performance. The advent of automated matching capability gives us the ability to improve matching performance and permit the deployment and use of new technologies in new ways to help us freeze or fix identities of foreign nationals, improve document security, and deter illegal access. To maximize our return on investment, it is vital that federal agencies and associated industries, who are also responsible for the security of infrastructure, work together to create compatible systems. US-VISIT has established a successful track record in protecting the integrity of the immigration and border management enterprise, but we continue to be vigilant in achieving our mission and goals.

US-VISIT is critical to our national security, and its implementation is already making a significant contribution to the efforts of DHS to provide a safer and more physically and economically secure America. We recognize that we still have a long way to go. We will build upon the initial framework and solid foundation to ensure that we continue to meet our goals to enhance the security of our citizens and visitors while facilitating travel for the millions of visitors we welcome each year.

Safeguarding Personal Privacy in General

The September 11 Commission Report recommends the creation of a board within the Executive Branch to oversee the balance of information sharing and privacy protections. We are working with other agencies to consider this recommendation. I can speak to the successes we have seen within DHS on privacy protections.

DHS has the first statutorily mandated Privacy Officer who serves the Department in two capacities. First, she works directly with operational components across the entire Department to embed privacy practices into the technology and the business processes DHS uses to accomplish its mission. To support this intense integration, the Privacy Officer also places privacy officers in the field, working side by side with the staff of DHS components. Second, she investigates and oversees DHS adherence to existing privacy laws and reports to both the Secretary and separately to Congress on DHS challenges and successes with privacy compliance. Through this dual role, the DHS Privacy Officer builds solid privacy practices into the daily work of the Department and assists in building a long term strategy for balancing privacy and security into the future. In its Report, the 9/11 Commission speaks of the need for creativity. The creation and the work of the DHS Privacy Officer is one example of how DHS is taking a new approach to providing comprehensive and balanced security to the nation.

Here in DHS, we can show the effectiveness of a strong privacy officer at the agency level and the success that is achievable only through direct integration of privacy protections and operational work. Privacy is an issue that stretches across the entire government and as we continue to look at government-wide approaches to privacy, it is also important to see how productive agency-level privacy protections are.

Interagency Human Trafficking Center

Last month, DHS and the Departments of State and Justice established the Human Smuggling and Trafficking Center. The center is housed at the State Department and includes the participation of intelligence agencies.

The Center analyzes and disseminates information, and provides related support to law enforcement, intelligence, diplomatic, foreign assistance, and other entities that take action against the threats of human smuggling and trafficking and against criminal support for terrorist travel.

The Center is another measure that the Administration has taken to improve our ability to analyze and disrupt terrorist travel. We are optimistic about its possibilities.

Targeted Prosecutions

DHS has coordinated an interagency working group to assure the greatest level of situational awareness for threat reporting, preparedness and coordination at all levels of government for the next several months. As part of this effort, ICE, CBP, and the FBI are working closely with the Department of Justice and the various United States Attorneys' Offices to identify, investigate, and criminally prosecute aliens possessing fraudulent documents, making false statements, or committing other immigration violations, where there is a suspicion of a connection to terrorism or a particular compelling national security interest.

All U.S. Attorneys' Offices were asked to meet with DHS and FBI representatives in their districts to develop guidelines for effective prosecutions in these cases and to articulate clearly the terrorism and national security interest at stake. The goal of the initiative is to ensure that the federal agencies are referring cases where a criminal prosecution can be brought to prevent and disrupt terrorism not to increase the number of criminal prosecutions for immigration violations.

An Integrated Screening System

The 9/11 Commission also recommended that, "[t]he U.S. border security system should be integrated into a larger network of screening points that includes our transportation system and access to vital facilities, such as nuclear reactors. The President should direct the Department of Homeland Security to lead the common effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind."

There is no one-size-fits-all system to screen all persons, at all times, for all purposes. Instead, DHS, other federal agencies, state and local agencies, and the private sector rely on multiple screening systems that serve unique functions. The systems we develop need not be the same, but they must be interoperable to the extent possible.

US-VISIT

Earlier, I described the border screening system that is used by US-VISIT. US-VISIT employs a continuum of security measures that begins before individuals enter the U.S. and extends through their departure from the country. At assigned U.S. border points of entry, designated visitors are required to provide biometric data, biographic data, and/or other documentation. This data is checked against various databases which contain visa issuance information, terrorist and criminal watchlists, and immigration status information allowing CBP Officers at the border to verify identity and identify criminals, security threats and immigration violators.

CBP and One Face at the Border

DHS has also unified our border inspection process under the Customs and Border Protection Officers, who are cross-trained to address immigration, customs, and agricultural inspection needs. We now have one face in one uniform where we used to have three.

CBP recently graduated the first class of officers who are trained to operate primary inspection in all three areas. These officers -- now trained in all three areas of inspection and armed with the best intelligence we have -- improve our ability to spot and stop terrorists quickly and keep them out.

Transportation Security Administration

It is very important to note progress already made by the U.S government in expanding the existing no-fly and selectee lists. Prior to 9/11, there were fewer than 100 names on the "no fly" list. Today, the Transportation Security Administration (TSA) provides carriers with "no fly" and "selectee" lists that have been dramatically expanded. Every day, intelligence and law enforcement agencies submit new names for consideration. This places a significant burden on air carriers, reservation systems and airline passengers, and we appreciate their efforts and patience as these lists are used and continue to expand. Continued expansion will be possible through the integration and consolidation of various watch lists by the Terrorist Screening Center (TSC), and as the U.S. Government is able to assume the responsibility for conducting the list comparisons.

After a significant review of TSA's proposed CAPPS II system, DHS is nearing completion of a next-generation passenger prescreening program that meets our goals of using the expanded no-fly and selectee lists to keep known or suspected terrorists off of planes; moving passengers through airport security screening more quickly; reducing the number of individuals unnecessarily selected for secondary screening, and most importantly, fully protecting passengers' privacy and civil liberties.

A revised program will likely incorporate the valuable lessons we have learned from existing passenger prescreening programs, remove the responsibility from air carriers for conducting watch list comparisons, and improve aviation security. We look forward to working closely with Congress, the privacy and civil liberties communities, and the aviation community to implement a new passenger prescreening program in the most cost-efficient and least-intrusive manner possible.

This summer, TSA initiated a pilot program, the Registered Traveler program, to help identify low-risk travelers. This program will allow screening resources to be more efficiently focused on higher-risk travelers.

The goal of the Registered Traveler (RT) Pilot Program is to use biometric technology in conjunction with pre-screening security assessments to assess the potential for an expedited screening procedure for qualified individuals. The RT concept is based on the premise that a balanced combination of terrorist threat analysis, verification of identity at the security checkpoint, and better-targeted physical screening can improve security and customer service. The RT Pilot Program is designed to allow DHS to focus its security resources on travelers that are "less known."

The program also includes a Registered Armed Law Enforcement Officer component to verify the identity of law enforcement officers who are traveling while armed.

I am pleased to announce we have launched operations at four of our five pilot locations: Minnesota, Los Angeles, Houston, and Boston which began operations on this past Tuesday. Washington DC's Reagan National Airport will launch operations in the next few weeks.

Additional Steps

We are continuously reviewing the systems that we have in place, and those under development. Our first priority is to ensure that the screening system works as intended. But we are also looking to see whether the system we employ in one place, for one function, can be used elsewhere.

I am leading a study within DHS to review the entire range of biometric programs that the Department employs. We want to see if it is possible to integrate the various screening programs and improve the performance of our mission functions. We are reviewing whether information we obtain in one program can be shared with another - without compromising the privacy rights and civil liberties of the individuals screened. That work is fully consistent with the Commission's recommendation in this area, and I am hopeful that it will lead to more efficient and integrated screening processes.

DHS Efforts to Strengthen Identity

I have testified above about the steps DHS has taken to strengthen the identification system used at our borders. For the very first time in our country's history, we are able to verify, through the collection and analysis of biometric information, that the foreign visitor who applies for and obtains a visa in the name of "Bill Smith" is the same "Bill Smith" who arrives at a U.S. port of entry.

DHS has worked with other federal agencies, including the Social Security Administration, and non-profit agencies, such as the American Association of Motor Vehicle Administrators (AAMVA) on identity issues, including proposals to strengthen procedures that are used to issue identification documents.

AAMVA recently completed a two-year effort to develop a security framework for strengthening the security of state-issued driver's licenses and identification cards. The AMMVA membership has not yet had the opportunity to ratify the recommendations, and State legislatures have also not had the chance to study the framework and consider what steps they would need to take to comply with the recommendations.

DHS is carefully considering the framework and its proposals. DHS encourages the States to review the framework as soon as practicable, and to take the appropriate actions necessary to increase the security of their identity issuing process.

DHS encourages the appropriate state and local officials to discuss these issues with their State Homeland Security Advisors and Governors. Steps to strengthen identity documents should be made a part of each state's homeland security strategy.

We are monitoring developments closely in this area, and are willing to work cooperatively with the States.

USA PATRIOT Act

I would also like to note the importance of the various provisions of the USA PATRIOT Act to the work of DHS and the BTS law enforcement agencies.

The PATRIOT Act began to tear down the walls that prevented our policy makers from having the benefit of intelligence analyses that were based on all available information. The PATRIOT Act has facilitated the ability of ICE, in coordination with the FBI, to query financial institutions quickly about terrorists and known money launderers. PATRIOT Act provisions have also enabled our investigators to investigate irregularities in the non-traditional financial system to close down unlicensed money remitters who may be funding terrorist activities. The PATRIOT Act has also expanded the authority of ICE to detain and remove terrorists from the United States.

I strongly support the President's call for Congress to renew those provisions of the Patriot Act that will otherwise expire next year. These tools are important as we build more integrated and coordinated homeland security, intelligence, and law enforcement communities.

Conclusion

I have described a number of steps that DHS has taken to improve our border screening and law enforcement efforts as a result of the September 11th terrorist attacks.

Our systems are better and more focused on terrorist prevention then they were before that fateful day. We can continue to improve the measures that we take and are committed to doing so.

The employees of DHS and the law enforcement agents, CBP Officers, air marshals, screeners, and others within my area of responsibility at the Directorate of Border and Transportation Security are working as hard as possible every day to prevent another act of terrorism. DHS is continuing to improve our understanding of the risks presented so that we can shift our resources as nimbly as possible to respond to the changing threat environment.