Statement for the Record

Rand Beers
Under Secretary
National Protection and Programs Directorate
Department of Homeland Security

Before the
United States Senate
Committee on Homeland Security and Governmental Affairs
Washington, D.C.

Terrorist Travel

December 9, 2009

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members, I am pleased to appear before you today to discuss the progress the Department of Homeland Security (DHS) has made in securing our Nation's borders. Our vision is to modernize and improve the immigration and border management system through integration, collaboration, and cooperation among all parts of the immigration and border management community, including U.S. Customs and Border Protection (CBP), U.S. Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) Program, and the Department of State (DOS), among many others. These organizations continue to work together to accomplish a single mission—coordinating roles, sharing information and technology, complementing and reinforcing one another's business processes, and eliminating redundancies and gaps.

For terrorists to plan and carry out physical attacks on our homeland, they must have access to our Nation. As the 9/11 Commission's Final Report states, "Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger because they must surface to pass through regulated channels to present themselves to border security officials, or attempt to circumvent inspection points … for terrorists, travel documents are as important as weapons."

When DHS was created after the terrorist attacks of 9/11, the Department's work to implement measures to identify and stop terrorist travel accelerated rapidly. Three areas received significant investment: 1) creating a biometrics-based screening capability that would also record the entry and exit of foreign citizens; 2) enhancing the security of travel documents; and 3) improving information sharing across Federal agencies to prevent the admission to the United States of known or suspected terrorists. I am pleased to tell you today that work on these three areas has made the Federal Government's traveler screening more collaborative, streamlined, and effective than ever before.

We have made significant improvements in the last five years:

- We have worked to unify immigration and border management systems in order to implement a robust, effective, timely and efficient capability to access and use biometrics-based information on criminals, immigration violators, and known or suspected terrorists.

- ICE identifies visitors who overstay their authorized terms of admission through an average of more than 300 credible leads that US-VISIT provides each week. Through ICE's Secure Communities program, we are also helping to identify immigration violators that state and local law enforcement officers arrest.

- Through the successful implementation of large scale biometric screening by US-VISIT we have provided support and leadership to biometric border management programs undertaken in the United Kingdom and Japan, and continue to support and encourage programs in various stages of application in the European Union, Canada, Mexico, Australia, Argentina, Peru, and other countries.

- We have put better capabilities in place for more efficient identification of fraudulent documents. We cooperated closely with DOS when it introduced an electronic passport, and we made every effort to ensure compliance with new passport standards by Visa Waiver Program countries. We have also worked together with State to implement the U.S. passport card, which provides U.S. citizens a secure, limited-use travel document in a more convenient format.

- We have implemented the Western Hemisphere Travel Initiative, whereby U.S. and Canadian travelers are required to present more secure travel documents that denote identity and citizenship when seeking to enter our country, helping officers focus on threats while making legitimate travel more efficient.

These are significant achievements that have improved national security and have impeded terrorist travel.

Biometrics-Based Screening: US-VISIT

The 9/11 Commission, Congress, and DHS all recognize that accurately documenting the entry and exit of non-U.S. citizens is a priority for securing our Nation's borders and improving the integrity of our immigration system. With biographic screening capabilities already well established, biometrics became the next logical step in the evolution of immigration and border management.

Two primary factors drive our use of biometrics. The first is the need to overcome the increasing sophistication of criminals and terrorists who are determined to circumvent our biographic-based security measures. The second factor is societal change—the public increasingly accepts the use

of biometric technology as an effective, convenient, and efficient means to guard against terrorism and fraud, including identity theft.

Biometrics addresses these factors because they provide a reliable and accurate way to establish and verify visitors' identities. Unlike names and dates of birth, biometrics is unique and difficult to forge. Biometrics helps us meet the challenge of making travel more difficult for those who want to do us harm, while making it convenient and efficient for legitimate visitors to come to the United States.

On January 5, 2004, DHS significantly advanced our Nation's border security by launching US-VISIT, a first of its kind, large-scale, biometrics-based identity and screening system, supporting the work of DOS consular and CBP officers who respectively make visa-issuance and admission decisions.

- Through its use of biometrics, US-VISIT provides identification and analysis services that help decision makers distinguish people known to pose a threat from the millions of people who travel with legitimate purpose. Biometric information is paired with biographic information to establish and verify an individual's identity; that identity is subsequently vetted against watch lists.

- US-VISIT checks a person's biometrics against a watch list of more than 4.7 million known or suspected terrorists, criminals, and immigration violators; US-VISIT also checks a person's biometrics against those DHS has on file associated with his/her travel document to ensure that the document actually belongs to the person presenting it. US-VISIT provides the results of these checks to decision makers when and where they need them.

The Department's implementation of biometric capabilities has laid the foundation for the rapid expansion of biometric identification to other agencies.

Identity and Screening Services for DHS and Other Agencies

In another effort to streamline DHS processes, the Department has designated US-VISIT's Automated Biometric Identification System (IDENT) as the biometric storage and matching service for the Department, providing biometric identification and analysis services to agencies throughout the immigration and border management, law enforcement, and intelligence communities. This information is collected to aid in determining whether foreign travelers: should be prohibited from entering the United States; can receive, extend, change, or adjust immigration status; have overstayed or otherwise violated their authorized terms of admission; should be apprehended or detained for law enforcement action; or need special protection or attention (e.g., refugees).

IDENT plays an important role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, USCIS, and the U.S. Coast Guard. US-VISIT also supports the DOS BioVisa Program and shares information with the Federal Bureau of Investigation (FBI).

Additionally, US-VISIT is working with a number of other DHS components, such as the Transportation Security Administration (TSA), on future and planned credentialing and identity-management programs.

Visa Overstay Process

In addition to enhancing security for visa-free travel, DHS is taking steps to identify individuals who have overstayed their terms of authorized admission.

US-VISIT Overstay Identification and Analysis

The Arrival and Departure Information System (ADIS) database was designed to match biographic data on arrivals, departures, extensions, and changes or adjustments of status to identify individuals who have overstayed the authorized terms of their admission.[1] The system provides an overstay status indicator and seeks to determine nonimmigrant status by assessing whether visitors have remained beyond their authorized terms of admission based on the "admit until" dates on the Arrival/Departure Record (I-94).

Immigration overstays fall into two categories: in-country overstays and out-of-country overstays. In-country overstays are individuals who have exceeded their authorized terms of admission by remaining in the United States. Out-of-country overstays are individuals who, according to the arrival and departure dates, have departed the United States, but who stayed beyond their authorized terms of admission by more than seven days for Visa Waiver Program participants or 180 days for those individuals issued a visa.

In-Country Overstay Summary

Records of individuals whose status indicates a possible in-country overstay are verified and validated by the US-VISIT Data Integrity Group (DIG). The records undergo a series of four automated searches, which historically reduce the number of overstay records by 40-45 percent. The remaining records are then manually verified and validated by DIG analysts to ensure that only credible leads are forwarded to ICE. During the manual DIG verification and validation process, additional government systems are checked. Records that cannot be closed after manual review are transmitted to ICE as in-country overstay leads.

Out-of-Country Overstay Summary

The DIG reviews and validates all out-of-country overstay records that ADIS identifies (regardless of priority or non-priority status). If the overstay is confirmed, the DIG creates both biographic and biometric lookouts in TECS (formerly known as the Treasury Enforcement Communications System) and IDENT for these individuals, which are then available to all TECS and IDENT users, including:

- CBP officers, when an individual attempts to enter at a port of entry;

[1]ADIS receives arrival/departure manifests (APIS), officer-confirmed arrivals (TECS), and changes/extensions/ adjustments of status (CLAIMS 3 and SEVIS).

- USCIS, if a person applies for an immigration benefit;
- ICE, if a person is encountered in an immigration enforcement context; and
- DOS consular officers, when an individual applies overseas for a visa to enter the United States.

10-Fingerprint Transition

DHS' transition from collecting two to collecting 10 digital fingerprints at U.S. ports of entry from visitors to the United States is nearly complete. DHS deployed new 10-fingerprint scanners at ports of entry in 2008, and today the new 10-fingerprint scanning devices are in place at all major ports of entry, where international visitors can expect to use the upgraded technology when they enter the United States.

The use of 10-fingerprint readers improves the accuracy of identification; improves interoperability with the FBI, DOS, and local and tribal governments; and reduces the number of travelers referred to CBP secondary inspection. DHS is now able to conduct full searches against the FBI Unsolved Latent File, which allows DHS to match against prints lifted from crime scenes and those collected on battlefields and in safe houses overseas.

Interoperability with the Departments of Justice and State

DHS' 10-fingerprint collection standard makes our system more compatible with the FBI's biometric system, the Integrated Automated Fingerprint Identification System, known as IAFIS. DHS, the Department of Justice (DOJ), and DOS signed a memorandum of understanding regarding interoperability on August 1, 2008. The first-phase capabilities for the initial operational capability were deployed in October 2008.

This integrated system will allow authorized users access to all relevant information in a timely manner so that they can make the right decisions about the individuals they encounter. The interoperability also benefits the FBI and other law enforcement organizations by providing them with increased access to immigration information about high-risk individuals to whom DOS has refused visas and those whom DHS has removed.

Developing Interoperability with the Department of Defense (DOD)

One of the Federal Government's greatest challenges is identifying the unknown terrorist—one who poses a threat but whose name is not known to us or who comes in under a false name. The tried and true method for identifying the unknown terrorist is the fingerprint. A latent fingerprint that is left on an object or in a terrorist training camp or safe house is, in fact, a powerful tool for determining who has been in that place or who has handled that object. The defense and intelligence communities collect these latent fingerprints.

DOD currently sends fingerprints to US-VISIT to be checked against the IDENT biometric watch list of known or suspected terrorists, criminals and immigration violators as well as the other individuals who have come in contact with DHS through immigration and border interactions. One of the results of the transition to 10-fingerprint collection is the increased

likelihood that we will identify the nameless suspect based on his or her immigration or criminal history regardless of the kind of fingerprint DOD finds.

As an example, a person accused of associating with a manufacturer of improvised explosive devices (IEDs) was detained by Coalition Forces in Iraq. The FBI and US-VISIT checked his fingerprints against their data, and US-VISIT fingerprint examiners connected the person detained to a fingerprint DOD had collected from electrical tape inside a piece of an IED. Based on that latent print identification made by US-VISIT, DOD increased the person's security threat level. DHS is now working to make US-VISIT's biometric system compatible with DOD's Automated Biometric Identification System, which will facilitate identification of terror suspects that U.S. forces encounter. Information on these individuals is in our systems in the event they attempt to apply for admission into the United States.

Biometric Exit

Developing an automated exit capability consistent with the recommendations of the 9/11 Commission and Congress has been a priority for the Department since the inception of the US-VISIT program. By adding biometrics to the current biographic-based system of recording departures, DHS will have a more accurate and efficient way to determine whether foreign citizens have departed the United States.

Air

DHS has performed significant planning and testing over the past three years to examine possible solutions for integrating US-VISIT biometric exit requirements into the international air departure process. For more than two years, US-VISIT ran biometric exit pilots at 12 airports and two seaports. These pilots evaluated the use of both automated kiosks and mobile devices in port terminals. When the pilots ended in May 2007, an evaluation determined that the technology worked effectively, but traveler compliance was low. DHS determined that biometric air exit needs to be integrated into the existing international traveler departure process.

On April 24, 2008, DHS published a notice of proposed rulemaking (NPRM) proposing that commercial air carriers and vessel carriers collect and transmit the biometric information of international visitors to DHS within 24 hours of their departure from the United States. Before finalizing the Air-Sea Exit NPRM, Congress, in the Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (Public Law 110-329), required us to test additional biometric collection to ensure that the best available procedures are implemented.

From May 28 to July 2, 2009, US-VISIT tested biometric air exit procedures at two airports: Detroit Metropolitan Wayne County Airport and Hartsfield-Jackson Atlanta International Airport. In Detroit, DHS tested the collection of passengers' biometrics at the boarding gate by CBP officers. In Atlanta, DHS tested the collection of passengers' biometrics at TSA checkpoints. The Department has submitted to the Committees on Appropriations of the Senate and the House of Representatives, as well as to the Government Accountability Office, an evaluation report of these pilots, consistent with Public Law 110-329. The results of the pilot

evaluation, combined with the review of public comments submitted in response to the NPRM, will inform the decision on the option to be selected for publication in the final rule.

Land

Biometrically recording the departures of non-U.S. citizens at U.S. land border ports of entry poses significantly greater challenges. Each year, our land border ports of entry see more than 300 million crossings at 170 port locations, including seasonal and other ports that are not open year round. Due to variations in infrastructure, environment, and traffic volume from port to port, a one-size-fits-all solution will be difficult. The Department is examining options for the land border environment that will not negatively impact the economy, the environment, or traveler safety.

International Cooperation and Collaboration

When DHS began the US-VISIT program to collect biometrics as part of port-of-entry inspection and screening, the world watched to see if the benefits of biometrics would work on a large scale. Although a handful of nations were testing biometrics, DHS was the first to launch a comprehensive, biometrically based identity-management system for immigration and border management, and we now serve as a model for countries developing similar systems.

Some countries have already begun operations or are nearing deployment. For example:

- Japan has implemented a two-fingerprint biometric entry system similar to US-VISIT's initial system;
- The United Kingdom is collecting 10 fingerprints from visa applicants and testing fingerprint collection at ports of entry;
- The European Union is building a 10-fingerprint visa-issuance program based on the very successful Eurodac;
- Australia, which has been a pioneer in facial recognition, is advancing its identity-management program;
- The United Arab Emirates has long been using iris scans as part of its immigration and border control processes; and
- Other countries, including Peru, Mexico, and Canada, are actively pursuing biometrics implementation.

As the use of biometrics increases worldwide, consistent international standards for biometrics and data sharing are essential to developing compatible systems, and compatible systems are essential to hindering international criminal enterprises as well as terrorists' ability to travel.

The Future of Biometric Screening

Biometric screening offers real opportunities to dramatically increase the efficiency of identifying people. The Department is already researching emerging technologies to expand our screening and identification capabilities, and we recognize that future systems will require increased assurance, efficiency, ease of use, and flexibility.

As DHS further evaluates biometric exit procedures, both at airports and land border ports of entry, we are looking for more efficient, less invasive technologies to verify visitors' departures. Particularly at the land border, we seek technologies that might meet our needs better than requiring visitors to have their fingerprints scanned while driving through a port of entry.

In some cases, the key to expanding biometric screening is to bring the technology to remote locations where decision makers need it. CBP's Air and Marine Operations is examining opportunities to use mobile biometrics in its areas of operation. The Coast Guard is using mobile biometric collection and analysis capabilities off the coasts of Puerto Rico and Florida, in coordination with US-VISIT. This has helped the Coast Guard identify and refer for prosecution and/or administrative immigration proceedings hundreds of repeat illegal migrants who are ineligible to enter the United States, including some wanted for human smuggling or murder.

Success Stories

Our many success stories include stopping more than 8,000 criminals or immigration violators at the ports of entry based on biometrics alone, and identifying thousands who are ineligible to receive visas to travel to the United States. No doubt, we have deterred countless more.

DHS' use of biometrics is helping disable the use of fraudulent or altered travel documents. For example:

- On March 16, 2008, a subject arrived at John F. Kennedy International Airport in New York and applied for admission with a valid Turkish passport and an unexpired B1/B2 visitor visa. He was referred to secondary inspection as a match to the IDENT biometric watch list for a previous voluntary departure. Secondary inspection revealed that on November 10, 2003, the subject had been apprehended taking pictures of the Ft. Leonard Wood Missouri Military Base. While in custody, it was discovered then that he had overstayed his authorized period of admission in the United States. The subject was now attempting to enter the United States using the identity of his twin brother and his brother's travel documents. The subject was denied access and is inadmissible to the United States for willful misrepresentation and not being in possession of valid travel documents.

- Biometrics is also helping at our borders away from ports of entry. In December 2007, the Coast Guard interdicted 10 migrants attempting to enter Puerto Rico illegally by sea. A check of the migrants' biometrics against IDENT revealed that two of the migrants had illegally entered the United States before, had been subsequently removed from the United States, and were suspected of being part of a human trafficking organization. The two suspected traffickers were brought ashore for referral for prosecution along with two witnesses who would testify against them. Since the adoption of the Biometrics at Sea System (BASS) in 2006, the Coast Guard has seen an 80 percent reduction in the number of migrants trafficking through the Mona Pass. The Coast Guard has collected over 2,500 biometrics signatures to date, with over 25 percent of those signatures returning a positive match, or "hit", resulting in over 250 successful prosecutions.

US-VISIT and Privacy

DHS is committed to adhering to the strictest privacy standards. DHS collects only the information needed to achieve program objectives and missions and restricts the use of this information to the purpose for which it was collected. DHS also conducts periodic audits of its systems to ensure appropriate use within the framework of the Privacy Act.

Ultimately, the success of the US-VISIT program will be measured not only by our ability to identify those who may present a threat, but also by our ability to protect against identity theft and fraud. We are acutely aware that our success depends on how well we are able to protect the privacy of those whose biometrics we hold. We have a dedicated privacy officer responsible for ensuring compliance with privacy laws and procedures and for creating a culture of privacy protection within US-VISIT. It bears mention that our policy also extends most of the same privacy protections afforded to U.S. citizens to non-U.S. citizens as well. From the beginning, we have emphasized that the information gathered by DHS or DOS will be used only for the purposes for which it was collected, consistent with those uses authorized or mandated by law. We regularly publish privacy impact assessments and system of records notices to provide the public with a clear view of the information we collect, how we store it, and our policies to ensure it is not abused.

Conclusion

Biometrics has increased our Nation's security and the security of nations around the world to a level that simply could not exist before. Biometrics affords us greater efficiencies and makes travel more convenient, predictable, and secure for legitimate travelers. Biometrics enables people to have greater confidence that their identities are protected, and in turn, decision makers are more certain that the people they encounter are who they say they are.

To ensure we can shut down terrorist plans before they ever get to the United States, we must also take the lead in driving international biometric standards. By developing compatible systems, we will be able to securely share terrorist information internationally to bolster our defenses. Biometrics provides a new way to bring terrorists' true identities to light, stripping them of their greatest advantage: anonymity.

So what is next?

We must aggressively pursue innovation. Those who want to do harm continue to search for ways to exploit our weaknesses, so we cannot afford to lag behind. We too must search for even more efficient and affordable identification technologies.

We also need to continue to advocate abroad. With the power of biometrics and a foundation of international cooperation, we can transform and enhance the way people travel the world and the way countries protect themselves from those who would do them harm.

The Department's use of biometrics plays a crucial role in supporting many programs and initiatives within DHS and other Federal agencies. Chairman Lieberman, Ranking Member Collins, and distinguished Members, we have outlined our current efforts that, with your assistance, will help DHS continue to protect our Nation.

Thank you again for this opportunity to testify. I will be happy to answer any of your questions.