Statement for the Record

Rand Beers
Under Secretary
National Protection and Programs Directorate
And
Coordinator for Counterterrorism
Department of Homeland Security

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

Terrorist Travel

July 13, 2011

Introduction

Chairman Lieberman, Ranking Member Collins, and distinguished Members, I am pleased to appear before you to address what the Department of Homeland Security (DHS) has done to prevent terrorists from traveling to the United States. Our goal is to push information to the frontlines at the earliest possible point to prevent known or suspected terrorists from traveling to the United States. Today, I am testifying in two capacities. I am testifying as the Under Secretary for the National Protection and Programs Directorate (NPPD), a position I was appointed to by President Obama and confirmed by the Senate in June 2009. In this role, I have responsibility for the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program and will speak to the tremendous work that organization is doing to validate identities and identify known or suspected terrorists. I am also testifying as the Coordinator for Counterterrorism at the Department, a role Secretary Napolitano assigned to me following the December 25, 2009, attempted bombing of Northwest Flight 253. I will address what the Department is doing to better coordinate its efforts to prevent terrorist travel, and describe the specifics of what US-VISIT activities are being done in this area. As this is my first testimony as the Counterterrorism Coordinator, I will also discuss why this role was created, how it has evolved, and the lessons the Department has learned since its creation.

Coordinating Terrorist Travel Screening

DHS collects and screens information on who is entering the country or boarding an aircraft in order to identify possible links to terrorist activity. U.S. Customs and Border Protection (CBP) has developed very sophisticated capabilities at the National Targeting Center as has the Transportation Security Administration (TSA) with Secure Flight. These advancements compliment the substantial progress that is being made across the federal government in accessing, sharing and vetting travel data. We continue to work closely with members of the

Intelligence and Federal Law Enforcement Communities to further enhance our ability to prevent known and suspected terrorist from entering our country.

In this regard, the Department has made considerable progress since 9/11 to implement measures to identify and stop terrorist travel including:

- Unifying immigration and border management systems to implement a robust, effective, efficient, and timely capability to access and employ biometric- and biographic-based information across the homeland security spectrum.

- Enhancing capabilities for more effectively identifying fraudulent documents and imposters and implementing measures to confirm document authenticity and validity.

- Establishing system interoperability and information sharing protocols with Federal partners and supporting State and local law enforcement agencies and the Intelligence Community. Working with our partners enables agencies to more effectively connect the dots and determine those who might pose a threat, through use of a more complete and accurate picture of a person's immigration, terrorist, and criminal history, as well as those that try to use more than one identity.

- Streamlining the visa overstay review process to establish reliable data on individuals who have violated the terms of their authorized admission.

- Establishing and maintaining strategic partnerships with an increasing number of international partners, sharing appropriate information, providing technical assistance, developing commonality in biometric standards and best practices, and investigating and testing emerging multimodal biometric technologies.

In the last few months, we have accelerated many of these efforts. In one notable example, the Secretary directed CBP, U.S. Immigration and Customs Enforcement (ICE), US-VISIT, U.S. Citizenship and Immigration Services (USCIS), Intelligence and Analysis (I&A), the Office of Policy, the Office of Operations Coordination and Planning (OPS), the Office of the General Counsel, the Privacy Office, and the Office of Civil Rights and Civil Liberties to come together to address the backlog of unvetted potential visa overstays identified by the Government Accountability Office 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 investigation and removal actions for those that may pose a threat to national security. Since this effort began, DHS has used automated means to determine that of the 1.6 million potential visa overstays GAO reported in April, 843,000 are no longer in the country or have adjusted status. The remaining 757,000 are being vetted in three ways:

- First, US-VISIT, CBP and ICE are undertaking an initiative to run the overstay leads, both current and historical, through CBP's Advanced Targeting System (ATS). ATS has the ability to automatically check the records of potential overstays against other databases that can indicate a change in immigration status or a departure from the United States. Leveraging ATS yields an additional advantage of allowing the department to

quickly gain greater insights on the background of overstay leads, which will assist ICE as it prioritizes leads with a potential nexus to a national security concern.

- Second, DHS will now provide overstay leads to NCTC to identify additional derogatory information held by the Intelligence Community.

- Third, DHS is now leveraging an existing data-sharing arrangement with the Intelligence Community to provide ICE with any additional matches of overstay leads with derogatory information.

This effort has helped to bring about a higher standard of review of overstay leads than previously existed, and at little cost. The process will allow ICE to better prioritize targets for investigation and removal. It is a prime example of how a coordination function can work in support of our operating components to better leverage information and capabilities spread across the Department and the interagency.

As part of the way ahead for DHS, we are focusing our efforts on improving information sharing, streamlining screening and vetting and identifying those who would do us harm while allowing the free movement of legitimate travelers. The Secretary, the Deputy Secretary and I look forward to working with you to make these improvements.

US-VISIT

Let me now address the work US-VISIT is doing to identify visitors to this country and to assist in the overall security of our immigration system. US-VISIT provides biometric identification and analysis services to distinguish people who pose a threat from the millions of people who travel for legitimate purposes. The program stores and analyzes biometric data—digital fingerprints and photographs—and links that data with biographic information to establish and then verify identities. US-VISIT's Automated Biometric Identification System, known as IDENT, is the Department's biometric storage and matching service, IDENT contains a watchlist of more than 6.2 million known or suspected terrorists, criminals, and immigration violators. This enables US-VISIT to provide homeland security decision makers with person-centric, actionable information when and where they need it, including at CBP primary screening where the fingerprints of all foreign nationals are run against the watchlist with results returned in under 10 seconds.

IDENT data, paired with biographic information from US-VISIT's Arrival and Departure Information System, support decision maker determinations as to 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, as in the case of refugees. IDENT plays a critical role in the biometric screening and identity verification of non-U.S. citizens for ICE, CBP, the State Department, USCIS, and the U.S. Coast Guard. US-VISIT is also working with other DHS components, such as TSA, to support their credentialing programs.

US-VISIT's IDENT is fully interoperable with the Federal Bureau of Investigation's (FBI's) 10-fingerprint-based Integrated Automated Fingerprint Identification System (IAFIS). Daily transactions of FBI fingerprint data shared between IAFIS and IDENT number in the tens of thousands, providing the capability for FBI and US-VISIT customers to simultaneously match biometrics against our system, our watchlist, and FBI data.

Enhanced interoperability with the FBI has enabled US-VISIT to launch the Rapid Response capability, which allows CBP officers to search and receive a response against the FBI's entire criminal master file of over 69 million identities in near real time during primary inspection. Rapid Response is operational at four air ports of entry and is planned for nationwide deployment at air ports of entry next fiscal year.

DHS is also working closely with DOD to increase information sharing and establish interoperability between IDENT and DOD's Automated Biometric Identification System (ABIS). We currently have manual methods for sharing data. This helps DOD identify foreign combatants and match latent fingerprints retrieved from objects such as IED fragments or collected from locations where terrorists have operated.

The goal is to have the U.S. Government's three largest biometric systems—those of US-VISIT, the FBI, and DOD—completely interoperable, enriching our data sets, making information sharing more seamless and the biometric-checking process automated and far more efficient. While interoperable, the systems will continue to be maintained and guided by each agency's respective policies, including those to ensure appropriate privacy safeguards are in place.

International Cooperation and Collaboration

DHS works extensively with foreign governments to increase information sharing in order to prevent terrorist travel at the earliest point possible. The Department is focused on sharing appropriate information, increasing system interoperability, providing technical assistance, and establishing commonality in data and biometric standards and best practices. For instance, we are:

- Working with Mexican federal police and immigration authorities to identify and stop dangerous people from transiting Mexico, enhancing efforts to combat transnational crime and confront organizations whose illicit actions undermine public safety, erode the rule of law, and threaten national security, and supporting Merida Initiative capacity building programs such as the incorporation of biometrics into Mexico Immigration's Integrated System for Migration Operations.

- Forging new partnerships with New Zealand, India, South Africa, the Republic of Korea, Germany, Spain, Greece, and the Dominican Republic to support their implementation of biometrics.

- Sending technical experts to the United Kingdom, Australia, Canada, and, soon, New Zealand, to help build biometric capabilities and develop more systematic methods for information sharing.

- Helping to implement Preventing and Combating Serious Crime agreements to formalize sharing of biometric and limited biographic data under the U.S. Visa Waiver Program with Germany, Spain and the Republic of Korea.

DHS will continue to expand international coalitions to protect our Nation in the face of evolving terrorist threats, an increasingly interconnected global economy, and growing transnational crime. Along with our partners, we view cooperation, collaboration, and information sharing as critical in reaching our common goals of enhancing global security while facilitating legitimate travel and ensuring access to our economies.

Success Stories

Interoperability and information sharing between agencies and international partners continues to yield significant results, as demonstrated by these success stories:

- On February 3, 2011, the Australian Department of Immigration and Citizenship submitted a batch of fingerprints under the High Value Data Sharing Protocol of the Five Country Conference for matching against IDENT. The fingerprints of a subject applying for asylum status in Australia matched an identity on the IDENT biometric watchlist as a known or suspected terrorist to the FBI's Terrorist Screening Database. US-VISIT contacted the FBI Counterterrorism Division and its Terrorist Explosives Device Analytical Center to confirm the subject's derogatory information. The FBI then notified Australian authorities. The individual was not granted his asylum status in Australia based on this information.

- In November 2010, US-VISIT assisted in a case regarding a Turkish man attempting to gain employment at a nuclear power plant. It was determined that the subject was using a false document under a false identity in an attempt to demonstrate his legal status to reside and work in the United States. The subject was subsequently arrested by local DHS law enforcement authorities as an overstay and placed into Federal custody awaiting removal proceedings.

- In October 2009, a vessel named *Ocean Lady* containing 76 undocumented males arrived off the coast of British Columbia, Canada. The intent of all individuals on board was to claim asylum status in Canada. The Canada Border Services Agency (CBSA) intercepted the vessel and worked with the ICE attaché in Ottawa to determine whether information on the identities of the individuals existed in U.S. systems. Pursuant to an existing agreement between CBSA and DHS, the asylum claimants' fingerprints were submitted to US-VISIT for a search. The fingerprint searches in IDENT identified matched to two subjects identified as known or suspected terrorists as members of the Liberation Tigers of Tamil Eelam. Both subjects had also previously applied for U.S. nonimmigrant visas in 2008 and had been denied.

The Role of the Coordinator for Counterterrorism

Following the attempted attack on December 25, 2009, Secretary Napolitano assigned me an additional duty within the Department to improve coordination among the operational components and to bring together the policy and intelligence components to support this effort. As the Department's Coordinator for Counterterrorism, I am responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices related to detection, prevention, response to, and recovery from acts of terrorism.

In November 2010, DHS stood up the Counterterrorism Advisory Board (CTAB) to further improve coordination on counterterrorism among DHS components. As the Coordinator for Counterterrorism, I serve as the chair of the CTAB with the Under Secretary of Intelligence and Analysis and the Assistant Secretary for Policy supporting the Board as Vice Chairs. Members include the leadership of TSA, CBP, ICE, the Federal Emergency Management Agency, the U.S. Coast Guard, USCIS, the United States Secret Service, NPPD, and OPS. The DHS General Counsel serves as legal advisor to the CTAB and is present at all meetings.

As additional support for the CTAB, in December 2010, the Department also established a counterterrorism working group, known as the CTWG, to support the Coordinator for Counterterrorism and appointed a Principal Deputy Coordinator for Counterterrorism.

Our mission is aligned with the Department's central mission: to prevent terrorist attacks and enhance security. The Coordinator for Counterterrorism, the CTAB and the CTWG serve as the connective tissue that brings together the intelligence, operational and policy-making elements within headquarters and the components. We rely on I&A to provide an understanding of the threat and to coordinate with the intelligence components within the Department and within the Intelligence Community. We then facilitate a cohesive and coordinated operational response through the CTAB and other mechanisms so that we can deter and disrupt terrorist operations.

The CTAB is both headquarters-driven and component-driven. Components have the opportunity to engage in the Secretary's priorities in an organized, coordinated fashion, but also use the CTAB to bring attention to their initiatives and priorities that need support from other components and headquarters. The CTAB fosters collaboration among components and provides situational awareness of what each component does and needs from each other during a high-threat scenario. Similarly, we work with the Office of Policy to address long-term strategy issues that come out of this process and work to implement those changes. Let me provide two examples of how this process has worked over the last few months, with the offer to provide greater detail in a classified setting.

A few months ago, the Intelligence Community identified a potential threat to the Homeland. Over a series of interagency meetings, it was agreed that some mitigation measures needed to be put in place. Working within the Department, we put together a risk assessment to determine the most cost-effective way to mitigate the threat in the near term and then worked with our interagency partners to implement these measures. Now, the Office of Policy is working with our partners in the interagency to develop a long-term strategy to address the threat.

Another example is how the Office of Policy engaged the Homeland Security Advisory Council to develop recommendations regarding the color-coded Homeland Security Advisory System. After the report was issued, Policy worked within the interagency to reach agreement regarding the development of a new system. In January 2011, the President directed the establishment of the National Terrorism Advisory System—or NTAS. Once the concept was finalized, the actual system was implemented and operationalized by the Coordinator for Counterterrorism, with the support of Operations Coordination and Planning within 90 days.

Soon after NTAS was up and running, we had the opportunity to test it following the death of Osama Bin Laden. While DHS did not issue an NTAS alert based on the threat of reprisal attacks or information obtained at Bin Laden's hideout, the CTAB met daily for the first week, sometimes multiple times per day. In each meeting, the CTAB considered whether any of the new threat information, when weighed against current preventative measures, met the threshold of being "imminent and actionable" to warrant the issuance of an NTAS alert. While none did, I&A worked closely with the FBI and our partners throughout the intelligence community to disseminate information as appropriate to the local law enforcement community and the private sector. Additionally, TSA engaged in extensive outreach efforts with airports, airlines, and freight carriers, and implemented a series of new security measures in the weeks following while CBP identified additional targeting measures to disrupt potential retaliatory attacks.

Conclusion

DHS has worked hard to stop terrorists before they ever get to the United States. As we continue to work to address today's complex challenges, we will look for innovative ways to bridge gaps between information, technology, and human decision-making. Working with our partners, using common technologies, standards, and best practices, and sharing critical information, will better protect us from those who seek to exploit our immigration systems.

By strengthening and increasing coordination within the Department, across the Federal government, and with our international partners, we will develop and implement comprehensive that make efficient use of limited resources. With the appropriate coordination and structure within DHS headquarters, we can better support our operational components as they work to enhance the security of our immigration systems while facilitating legitimate travel. In my role as Coordinator for Counterterrorism for the Department, I look forward to continuing to work with you to evolve this role and address the challenges that remain.

Chairman Lieberman, Ranking Member Collins, and distinguished Members, thank you again for this opportunity to testify. I will be happy to answer any of your questions.