



**Statement for the Record**

**John D. Cohen  
Principal Deputy Coordinator for Counterterrorism  
United States Department of Homeland Security**

**before the**

**United States House of Representatives**

**Committee on Homeland Security  
Subcommittee on Border and Maritime Security**

**on**

**“Ten Years after 9/11: Can Terrorists Still Exploit our Visa System?”**

**311 Cannon House Office Building  
Washington, D.C. 20515**

**September 13, 2011**

## **Introduction**

Chairman Miller, Ranking Member Cuellar, and distinguished Members, I am pleased to appear before you to outline the efforts of the Department of Homeland Security (DHS) to both prevent terrorists from entering the United States and ensure that our Visa System is secure.

I am testifying today in my role as the Principal Deputy Coordinator for Counterterrorism (CT) at the Department. In this capacity, I will address the Department's efforts to enhance the security of the Visa System, and also discuss the creation and evolution of the CT Coordination functions at DHS. In addition, I will describe specific actions being taken by the National Protection and Programs Directorate's (NPPD's) United States Visitor and Immigrant Status Indicator Technology (US-VISIT) Program to complement the efforts of U.S. Immigration and Customs Enforcement (ICE) and U.S. Customs and Border Protection (CBP), alongside whom I am pleased to be testifying today.

## **Enhancing Visa Security to Prevent Terrorist Travel**

The Homeland Security Act of 2002 gave DHS the responsibility of preventing terrorists from entering the United States, providing the Department with the authority to establish and administer the rules that govern the granting of visas. This includes ensuring that the visa process is secure. Under this authority, DHS works closely with the Department of State to use the Visa System as a first layer of security to prevent known or suspected terrorists from traveling to the United States. Central to this mission is ensuring that consular officers at the State Department have necessary information, and then appropriately vet this information, which includes fingerprints and photographs, through the Department and our interagency partners.

Since 9/11, DHS has enhanced our nation's ability to detect individuals seeking to exploit the visa system through recurrent vetting of visa holders. In May 2010, CBP's National Targeting Center-Passenger (NTC-P) implemented a new program to conduct continuous vetting of U.S. non-immigrant visas that have been recently issued, revoked and/or denied. The Visa Hot List vetting ensures that changes in a traveler's visa status are identified in near real time. If a violation is discovered, and the person is scheduled to travel to the U.S., CBP will request that DOS revoke the visa and recommend to the airline that the person be denied boarding. If no imminent travel is identified, CBP will coordinate with DOS for a visa revocation, if appropriate. If the subject of an existing visa revocation initiated by the DOS or recommended by CBP is found to be in the United States, CBP will notify the Counterterrorism and Criminal Exploitation Enforcement Unit for further action.

In addition, since December 25, 2009, we have accelerated our efforts to synchronize, streamline, and advance the Department's overall vetting capability, which both increases security and efficiency. In particular, the Department is currently working to enhance screening efforts for those who have potentially overstayed their period of admission and modernize and enhance the Department's Biographic Exit architecture.

In May 2011, at the direction of Secretary Napolitano, DHS's CT Coordinator organized an effort to ensure that all overstays, regardless of priority, receive enhanced national security and public safety vetting by the National Counterterrorism Center (NCTC) and CBP.

NPPD/US-VISIT used automated means to review all records in the backlog by checking ADIS, CLAIMS, and I-94 holdings to reduce the backlog. As a result of this review, we identified 843,000 visa overstays who were no longer in the country. Then, both NCTC and CBP vetted the remaining 757,000 potential in-country overstay leads, along with 82,000 previously vetted overstay leads. CBP used its Automated Targeting System to query multiple databases, and to compare records to CBP's intelligence-based threshold targeting rules to identify indicators such as suspicious travel patterns or irregular travel behavior. Simultaneously, NCTC vetted the backlogged records through a number of databases held by the Intelligence Community.

By the end of July 2011, all of the previously un-reviewed possible overstays records had been reviewed from a national security and public safety standpoint and ICE is currently pursuing leads that meet our priorities.

This effort has increased the standard of review of overstay leads, at reduced cost. The process allows ICE to better prioritize targets for investigation and removal. It is a prime example of how increased coordination can help our Department to better leverage information and capabilities spread across the Department and the Federal government.

The Department is nearing the final stages of developing a plan that not only institutionalizes these vetting enhancements, but also improves the current biographic exit system as well. We are focusing our efforts on improving information sharing, streamlining screening and vetting, and ensuring identification of potentially harmful individuals.

This plan includes many enhancements, including those which will allow DHS to:

- Quickly identify and forward to ICE investigators overstays that are of a national security concern.
- Integrate and leverage relevant CBP, ICE and US-VISIT information systems and operational processes to automate manual data queries and to vet DHS held immigration and travel related information against a broad array of law enforcement and IC data holdings
- Incorporate an enhanced vetting capability that aggregates information from multiple systems into a unified electronic dossier reducing the need for US-VISIT researchers and ICE Agents to review multiple systems during their Validation and Vetting processes
- Take action against all overstays. DHS will forward information to the State Department for the purpose of cancelling visas of those who overstay. DHS will also eliminate the ability of those who overstay from using the Visa Waiver Program by cancelling any ESTA approvals or denying ESTA submissions for those who have overstayed. DHS will also place lookouts on individuals who overstay beyond certain statutory-identified time limits, so that they are inadmissible to the United States. DHS believes this will create a deterrent effect.

- Provide to Congress country-by-country data on percentages of nationals who have overstayed their period of admission.

DHS is committed to working with Congress to make these improvements.

In addition to improving visa security, DHS has also implemented other measures to prevent another terrorist attack, including:

- Unifying immigration and border management systems to implement a more effective capability to access and employ biometric- and biographic-based information when reviewing possible terrorist travel.
- Enhancing capabilities for identifying fraudulent documents and imposters and implementing measures to confirm the authenticity and validity of travel documents.
- Establishing interoperability and information sharing protocols with our Federal partners.
- Supporting state and local law enforcement agencies and the Intelligence Community; using a more complete and accurate picture of a person's immigration, terrorist, and criminal history enables DHS to more effectively make connections in determining who might pose a threat or use more than one identity.
- Establishing and maintaining strategic partnerships with an increasing number of international partners. In these partnerships, we share appropriate information, provide technical assistance, develop commonality in biometric standards and best practices, and investigate and test emerging biometric technologies.

### **The Role of the Coordinator for Counterterrorism**

Following the attempted bombing of Northwest Flight 253 on December 25, 2009, Secretary Napolitano gave NPPD's Under Secretary Rand Beers the additional role of CT coordinator. The Department's CT Coordinator is responsible for coordinating all counterterrorism activities for the Department and across its directorates, components, and offices related to the detection, prevention, response to, and recovery from acts of terrorism.

In November 2010, DHS established the Counterterrorism Advisory Board (CTAB) to further improve coordination on counterterrorism among DHS Components. As the CT Coordinator, Under Secretary Beers serves as the chair of the CTAB, with the Under Secretary of Intelligence and Analysis (I&A) 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 (FEMA), the U.S. Coast Guard (USCG), USCIS, the U.S. Secret Service (USSS), NPPD, and the Office of Operations Coordination and Planning (OPS). The DHS General Counsel serves as legal advisor to the CTAB.

In December 2010, the Department also established a counterterrorism working group, known as the CTWG, to support the CT Coordinator, and Secretary Napolitano later appointed me as Principal Deputy CT Coordinator.

The CTAB's mission is aligned with the Department's central mission: to prevent terrorist attacks and enhance security. The CT Coordinator, the CTAB, and the CTWG serve as the connective tissue that brings together the intelligence, operational, and policy-making elements within DHS Headquarters and the Components.

We rely on I&A to provide an understanding of potential threats and to coordinate with intelligence components within the Department and Intelligence Community. We then facilitate a cohesive and coordinated operational response, through the CTAB and other mechanisms, to deter and disrupt terrorist operations.

The CTAB is both headquarters and component driven. Components have the opportunity to address 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 headquarters and other components. In addition, the CTAB fosters collaboration among Components and provides situational awareness of what each Component does and needs during a high-threat scenario. Similarly, we work with the DHS Office of Policy to address day-to-day and long-term strategy issues identified through this process and work to implement those changes.

Let me provide the following examples of how this process has worked over the last few months, with the offer to provide greater detail in a classified setting.

### **NPPD/US-VISIT**

One of NPPD/US-VISIT's most important roles is to identify visitors to this country and to assist in the overall security of our immigration system.

NPPD/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. NPPD/US-VISIT's IDENT, is the Department's biometric storage and matching service.

IDENT contains a watch list of more than 6.2 million known or suspected terrorists, criminals, and immigration violators. This capacity enables US-VISIT to provide homeland security decision makers with critical information when and where they need it. For example, this system can be utilized during by CBP primary screening during to run the fingerprints of foreign nationals against the watch list, with results returned in fewer than 10 seconds.

IDENT data, paired with biographic information from NPPD/US-VISIT's ADIS, supports 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. Through ADIS, NPPD/US-VISIT can identify individuals who have overstayed their period of admission and then forward these leads to ICE for further action. In addition, IDENT plays a critical role in the biometric screening and identity verification of non-U.S. citizens for the State Department, ICE, CBP, USCIS, and the U.S. Coast Guard.

NPPD/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 NPPD/US-VISIT customers to simultaneously match biometrics against our system and watch list, as well as FBI data.

Enhanced interoperability with the FBI has enabled NPPD/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 more than 69 million identities, in near real-time, during primary inspection. Rapid Response is operational at four air ports of entry and is planned for nation-wide deployment at air ports of entry next fiscal year.

DHS is also working closely with the Department of Defense (DOD) to increase information sharing and establish interoperability between IDENT and DOD's fingerprint database, the Automated Biometric Identification System. We currently have manual methods for sharing this data, which has helped DOD identify foreign combatants and match latent fingerprints retrieved from objects such as improvised explosive device 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 NPPD/US-VISIT, the FBI, and DOD—completely interoperable, thereby enriching our data sets by making information sharing more seamless and automating the biometric-checking process to make it far more efficient. Even after complete interoperability has been achieved, the three systems will continue to be maintained and governed by each agency's respective policies, including those that ensure appropriate privacy safeguards are in place.

## **International Cooperation and Collaboration**

DHS works extensively with foreign governments to increase information sharing 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 to 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. DHS has supported non-intrusive inspection equipment training, financial crimes investigative training, canine enforcement

training, assistance in transitioning the Mexican Customs from a revenue-based institution to a law enforcement-based institution, and improvements in immigration control programs.

- 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 biometric systems.
- Sending technical experts to the United Kingdom, Australia, Canada, and, potentially, New Zealand, to help build biometric capabilities and develop more systematic methods for information sharing.
- Implementing the 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, the Republic of Korea, and other countries.
- Working with the International Civil Aviation Organization, the International Transport Association and INTERPOL to support the exchange of information and best practices and the establishment of standards in the areas of aviation security, identity management, emerging technologies, document security and verification, and fraud detection.

The Immigration Advisory Program (IAP) is another example of partnership between the Department, foreign governments, and commercial air carriers to identify and prevent high-risk, improperly-documented travelers from boarding US-bound flights. IAP is currently in operation at eight airports in six countries. IAP officers have established strong working relationships with foreign law enforcement and counterterrorism officials and facilitated a direct link and real-time communication between foreign counterparts, the U.S. Embassy/Consulate, and the National Targeting Center.

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**

Information sharing among 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 in Australia matched an identity on the IDENT biometric watch list as a known or suspected terrorist in the FBI's Terrorist Screening Database. DHS 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 asylum status in Australia based on this information.

- In November 2010, DHS assisted in a case involving an applicant for 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 DHS law enforcement authorities as an overstay and placed into Federal custody awaiting removal proceedings.
- In October 2009, a vessel named *Ocean Lady*, transporting 76 undocumented persons, 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 NPPD/US-VISIT for a search. The fingerprint searches in IDENT identified two subjects as known or suspected terrorists and 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. Both subjects were denied asylum in Canada.

## **Conclusion**

DHS is working 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 in 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. DHS is also cognizant that although physical security is of paramount concern and it is vital that we do everything possible to prevent terrorist travel, we must steadfastly seek to ensure that privacy, civil rights and civil liberties are always protected. In developing and operating our programs, the Department's Office of Privacy and Office of Civil Rights and Civil Liberties are an integral part of the process.

By strengthening and increasing coordination within the Department, across the Federal Government, and with our international partners, we will develop and implement comprehensive measures 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 Principal Deputy CT Coordinator for the Department, I look forward to continuing to work with you to address the challenges that remain.

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