

Testimony of

Ms. Elaine Dezenski

March 14, 2005

Statement of

Elaine Dezenski

Acting Assistant Secretary for Border and Transportation Security Policy and Planning

And

Thomas J. Walters

Assistant Commissioner for the Office of Training and Development
Customs and Border Protection

Border and Transportation Security Directorate

U.S. Department of Homeland Security

Senate Committee on the Judiciary

Subcommittee on Immigration, Border Security and Citizenship
and
Subcommittee on Terrorism, Technology and Homeland Security

"Strengthening Enforcement and Border Security: The 9/11 Commission Staff Report on Terrorist Travel"

March 14, 2005

Chairman Cornyn, Ranking Member Kennedy, Chairman Kyl, Ranking Member Feinstein, and distinguished Members, we are pleased to be here today to testify about the role of the Department of Homeland Security (DHS) in visa policy, improvements in the visa process, and training for border officers.

The 9/11 Commission reported that the visa issuance process was exploited to accomplish the September 11 attacks on the United States. The Commission recommended that the U.S. Government consider new approaches to combating vulnerabilities in the visa system.

The Secretary of DHS is vested exclusively with all authorities to issue regulations with respect to the Homeland Security Act of 2002 (the Act) and of all other immigration and nationality laws, relating to the functions of consular officers of the United States in connection with the granting or refusal of visas. Per the Act, DHS's responsibility for visa policy is exercised under the terms of a Memorandum of Understanding (MOU) between DHS and the Department of State (DOS) which was signed by Secretary Ridge and Secretary Powell on September 26, 2003.

The Border and Transportation Security (BTS) Directorate is responsible for overall visa policy at DHS. BTS has been working with DHS's Citizenship and Immigration Services (CIS) as well as the Departments of State and Justice to address United States' security interests in the visa issuance process to ensure that visas are issued only to those

eligible consistent with applicable law. We have also worked to integrate visa issuance policy into the larger spectrum of programs designed to secure international air travel and U.S. ports of entry.

Visa Policy

We have worked closely with DOS on specific visa policy issues since the MOU was signed. Over the past months, DHS and DOS have made a tremendous effort to combat the perception that security measures implemented since September 11 have made it too difficult for legitimate travelers to come to the United States. DHS recognizes that travel facilitation for students, scientists, tourists, and business visitors to the United States is crucial to the vitality of our economy and society and spreading democratic ideals, furthering scientific development, and promoting the image of America overseas. Working with the DOS we have examined how we can change policies to facilitate travel at the same time increasing security.

Under the Homeland Security Act and the MOU and subject to certain exceptions, DHS establishes visa policy and has final authority over DOS-initiated visa guidance involving the following: alien admissibility and any applicable waivers; visa classification, and documentation; place of visa application; personal appearance/interviews; visa validity periods; and the Visa Waiver Program.

DHS and DOS have also focused on making appropriate changes to streamline the Security Advisory Opinion (SAO) process while maintaining the security benefits it provides. Working with the DHS's ICE Visa Security Unit (VSU), BTS is considering how to improve electronic transfers of information and whether imposing reasonable deadlines on other agencies to review the underlying visa application is appropriate. We are also considering creating an interagency process to review criteria used in the SAO process.

Visa Security Functions and Accomplishments

Section 428 of the Act assigns DHS very specific visa security functions. The Act authorizes DHS to assign officers to each diplomatic and consular post at which visas are issued, and to conduct specific functions at those posts, including:

- ? providing expert advice and training to consular officers regarding specific security threats relating to the adjudication of visa applications;
- ? reviewing visa applications; and
- ? conducting investigations with respect to consular matters under the jurisdiction of the Secretary.

In addition, the Act requires that on-site DHS personnel review all visa applications in Saudi Arabia. It also authorizes DHS to establish permanent positions at overseas diplomatic or consular posts to participate in the terrorist lookout committee operating at post, and vests the Secretary of Homeland Security "with all authorities to issue regulations with respect to, administer, and enforce the provisions of the [INA], and of all other immigration and nationality laws, relating to the functions of consular officers of the United States in connection with the granting or refusal of visas..."

BTS has made substantial progress in implementing Section 428. Among the organizational accomplishments, BTS has:

- ? developed a headquarters organizational structure and assigned functional responsibilities including procedures for in-depth vetting of subjects of interest identified through visa security activities;
- ? established visa security review procedures and built a database to track visa security review workload;
- ? developed an academy-based Visa Security Officers (VSO) pre-deployment training program;
- ? established and maintained visa security operations at two posts in Saudi Arabia, which review 100% of the applications in that country, obtaining program funds and selecting permanent VSO's; and
- ? evaluated and selected, with DOS Bureau of Consular Affairs, five overseas posts for the next expansion.

Consular Officer Training and Performance

Consular training encompasses both formal and informal training activities. DHS is currently developing a formal training program for consular officers in consultation with the U.S. Immigration and Customs Enforcement (ICE) Office of Training. Informal training occurs on a regular basis at the two Saudi posts and will continue to be a critical form of consular training as the Visa Security Program (VSP) expands. Informal training involves day-to-day interactions between VSOs and individual consular officers. The VSOs share their law enforcement expertise and

immigration experience with the consular officers to guide their interviews and refine document review methods. Informal training also generates valuable input to VSU about the types of formal training consular officers may need.

With regard to the development of performance standards for DOS's use in evaluating consular officers, DHS views its role as an auditing function of DOS' own evaluation practices. VSU recognizes that its recommendation of performance standards as a basis for such an audit is dependent upon developing a sophisticated understanding of basic consular officer training, of how consular officers currently are evaluated, and of operating practices and skill sets at multiple posts. DHS intends to deploy additional VSOs to overseas posts and send VSU staff to DOS training, thereby enabling VSU to work with DOS to develop performance standards in FY2005.

VSP operations in Saudi Arabia, which began in October 2003, have yielded notable successes. The VSOs and consular officers have developed very cooperative and collaborative working relationships. The VSOs review all applications after the consular officers have completed their adjudication and made a decision whether to issue or deny the visa. In Fiscal Year 2004, DHS VSOs in Saudi Arabia reviewed approximately 21,000 visa applications. Additionally, the consular officers regularly ask the VSOs for assistance during the adjudication process, for example: to review an application, to clarify a question of immigration law, to review suspect documents, and to clarify or interpret derogatory information received about the applicant. In addition to ensuring rigorous scrutiny of visa applications, this practice provides an opportunity for on-the-job training of junior consular officers to enhance their skills in such areas as interview techniques, imposter detection, and fraudulent document identification. DHS officers also assist other law enforcement and intelligence entities at post in a range of areas, conduct liaison with host country officials, and initiate domestic investigations arising from visa security and investigative findings.

Security Advisory Opinion Process

In general, the SAO process provides an interagency review of visa applications selected based on defined risk criteria (established under various SAO category designations) or because they otherwise warrant further scrutiny (based on consular officer discretion). SAO processes are based on grounds of ineligibility found in the Immigration and Nationality Act, including those listed under Section 212(a) and 212(f). Three TDY DHS officers are assigned to the VSP at headquarters. These officers leverage DHS assets and assist in resolving problem cases. These officers investigate and recommend resolution on cases for which other interagency partners disagree.

Section 306 Cases

VSP also investigates visa applicants from State Sponsors of Terror (Cuba, Iran, Libya, North Korea, Sudan, Syria) to determine if they pose a threat to national security. The DHS-State MOU describes the role of each agency in handling Section 306 cases and the final "no-risk" determination under the Act is made by the Secretary of State Visa Waiver Program

The Visa Waiver Program (VWP) enables citizens of certain countries to travel to the United States for tourism or business for ninety days or less without obtaining a visa. While the VWP encourages travel and trade with our allies, it also makes the program attractive to those wishing to avoid visa-security checks conducted at U.S. consulates abroad. To mitigate the vulnerability posed by the misuse of the VWP as of September 30, 2004, DHS began to enroll VWP applicants in US-VISIT. This step narrowed security gaps by providing biometric watchlist checks and identity verification for subsequent visits to the United States.

The Enhanced Border Security and Visa Reform Act (EBSA) of 2002 required that beginning on October 26, 2004, VWP countries each certify that they have a program in place to issue their nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers that comply with International Civil Aviation Organization (ICAO) standards as a condition of continued participation in the VWP program. The law also required that visitors coming to the United States under the VWP present machine-readable, tamper-resistant passports that incorporate biometric and document authentication identifiers, if the passport is issued on or after October 26, 2004. Furthermore, DHS is required to install equipment and software at all ports of entry to allow biometric comparison and authentication of these passports. The Congress enacted a one-year extension of the deadline for both VWP travelers to use biometric passports and for the U.S. Government to install the equipment to read the passports. The new deadline is now October 26, 2005.

By law, DHS is required to review all participating countries periodically for continued participation in the VWP and report to Congress. Several countries (Slovenia, Belgium, Italy, Portugal, Uruguay, and Argentina) were reviewed by the legacy Immigration and Naturalization Service (INS), and two (Argentina (2002) and Uruguay (2003)) were

removed from the program. DHS, in coordination with the Department of State, is finalizing the current reviews for the remainder of the countries. This is the first comprehensive review of the countries and will form the "baseline" for future reviews.

US-VISIT

Prior to the terrorist attacks 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 focus on biometric technology as a means to verify the identity of foreign travelers. DHS established the US-VISIT program, and began implementing US-VISIT, as required, at 115 airports and 14 seaports of entry on January 5, 2004. In accordance with direction from the Secretary, biometric technology was incorporated into US-VISIT even though biometrics were not statutorily mandated by that date.

In addition to developing an integrated system that records the arrivals and departures of travelers and uses biometric technology to combat fraud, DHS is designing US-VISIT to: (1) provide information to U.S. Customs and Border Protection (CBP) Officers and DOS 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 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 the U.S. Government to:

- ? Conduct appropriate security checks: We conduct checks of visitors against appropriate lookout databases, including the TSDB, 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.

With US-VISIT, DHS and DOS together have created a continuum of identity verification measures that begin overseas, when a traveler applies for a visa, and continues upon entry and exit from this country. The system securely stores biometric and biographic data and uses travel and identity documents to access that information for identity verification and watchlist checks. As mentioned, on September 30, 2004, we began enrolling nationals from Visa Waiver Program (VWP) countries in US-VISIT when they travel to the United States and on December 29, 2004, US-VISIT was rolled out to the 50 busiest land border ports of entry.

At designated U.S. border points of entry, certain visitors, as have been determined by regulation, 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 (through the Terrorist Screening Database (TSDB)) and criminal watchlists, and immigration status information. That information allows a CBP Officer at the border to verify the identity of the traveler and check terrorist, criminal, and immigration violator watchlists. Since January 5, 2004, 20.5 million entries have been recorded through US-VISIT and 471 criminals and immigration violators have been denied entry based on biometric information.

SEVIS

Among the millions of travelers who arrive in the United States each year are nearly a million students and exchange visitors who come to attend school and to experience the American way of life. The former INS historically did very little to track them. Data on foreign students was not automated or centralized, and remained in paper form with the schools. INS had little idea whether those entering on student visas actually attended school or remained in status.

Pursuant to Congressional requirements, the INS began developing automated tracking systems for students in the early 1980s. The first system developed was the Student/School system. Vulnerabilities identified in that system were corrected by the current Student and Exchange Visitor Information System (SEVIS) which became operational in 2003. It is fully functional at this time. It has enhanced homeland security by allowing real-time access to data on all foreign students and exchange visitors in the country. It has permitted DHS to ensure that only legitimate students are admitted, and to better track their entry and exit. SEVIS has had the corollary benefit of reducing visa application and immigration fraud. ICE has made some 560 arrests of foreigners who violated their student immigration status.

Training

DHS has established a comprehensive training plan for our CBP Officers, Agriculture Specialists, and Border Patrol Agents. Carrying out the nation's homeland security mission requires a workforce with the necessary skills and proficiency to fight terrorist threats while effectively carrying out our traditional missions of interdicting drugs, intercepting illegal immigrants, and facilitating legitimate trade and travel.

New CBP Officer training

Since 9/11, we have developed an integrated curriculum for new CBP Officers. There are 3 specific components to the way new CBP Officers are trained: Pre-Academy, Academy Basic training at Glynco, GA, and post-Academy training conducted at the Ports of Entry (In-port training).

Before attending the Academy, trainees spend up to 30 days at their duty station undergoing both formal classroom and on-the-job training to provide them with a familiarity of their duties and the work environment. New officers now complete a 73-day training regimen which includes anti-terrorism, passenger processing, agriculture fundamentals, immigration, document examination, and customs cargo processing.

Another important addition to integrated CBP Officer basic training is our use of practical exercises throughout a trainee's 15 weeks at the Academy. In FY 2000, the Academy, in concert with the Federal Law Enforcement Training Center, established a full-sized, fully equipped model Port of Entry at the Federal Law Enforcement Training Center in Glynco, Georgia. Interviewing labs require trainees to practice observational skills and questioning skills, while applying their job knowledge of documentation requirements, immigration issues, customs exemptions, prohibited and restricted articles, and agricultural issues.

Trainees also receive 25 hours of formal instruction in Non Intrusive Inspection (NII) devices. In the automated information systems training, instruction has been expanded to 61 hours and stresses how the various systems used in CBP can help our anti-terrorism efforts. At the end of the training, students are graded in two practical exercises - one for the passenger-related systems and another for trade-related systems.

In-port training commences soon after the trainees return to their Ports of Entry. This portion of standardized training combines formal classroom and on-the-job training to develop the competencies required to successfully perform more complicated secondary functions.

Training for the Incumbent Workforce

CBP realized it needed to unify and integrate its existing operations and workforce. At the Ports of Entry, 18,000 inspectors came together from 3 different agencies. While new officers receive a wide range of intensive training during their first two years, the incumbent inspectors complete training based on operational priorities and workforce needs.

CBP has developed an immigration-focused curriculum called Unified Primary Cross Training as part of the training that CBP Officers need to have. Cross-training modules are being delivered at ports of entry all over the country. This training is being conducted by Field Training Officers from the CBP officer ranks with operational as well as training backgrounds. Incumbent CBP officers are expected to undergo cross training on an as-needed basis as determined by operational requirements prior to performing any new function.

Fraudulent Document Training

One of the specific areas addressed in the 9/11 Commission Report was fraudulent documents training. Under our new curriculum, our basic trainees receive 16 hours in fraudulent document training at the Academy that culminates with a graded practical exercise during which trainees examine characteristics of unique documents and determine if the documents are genuine, counterfeit or altered. The course highlights fraud indicators that may be present in evaluating any document for authenticity. Security features of U.S. entry documents and imposter detection are emphasized as well. Trainees that fail to successfully complete the course are removed from training. All instructors teaching this course have received training from the Forensic Document Lab.

In early 2004 CBP, working with the Forensic Document Lab (FDL) in McLean, Virginia, developed and presented an 8-hour fraud document class at all Ports of Entry. We currently have several FDL trained officers in every major field office within CBP.

FDL teaches a 3-day intensive train the trainer session for the Offices of Field Operations and Border Patrol on fraudulent document detection. The FDL assist s our frontline officers with any forensic document analysis, provides training, and issues intelligence alerts about current fraudulent document trends as needed, and does so on a recurring basis. The FDL also created a Pocket guide reference to Document Security Features and Printing Techniques that we sent to all frontline officers. CBP constantly changes training in the field as new information is discovered.

Anti-terrorism training

CBP developed a Counter-Terrorism Response (CTR) protocol and training to address questioning and detaining possible terrorist subjects. CBP also has a Detecting Deception and Eliciting Reponses (DDER) Course which is advanced training in non-coercive interviewing techniques and includes a day of classroom lectures on such topics as Behavioral Analysis and Interviewing Strategies, followed by 2 days of CBP specific "role playing" exercises. The primary focus of the DDER course is to enhance the CBP Officers' questioning skills and to build upon the officers' arsenal of interviewing techniques while confronting potential terrorists.

Conclusion

We have made much progress to deny terrorists the ability to travel freely into the U.S., identify potential people smugglers, and constrain the mobility of known and suspected terrorists. In addition to the initiatives described above, we are working aggressively with our international partners to improve standards for travel documents, enhance aviation safety and port security, and speed the exchange of terrorist identifying information. DHS understands that we must engage in a global effort each day, through collaboration, information sharing and ongoing dialogue to bring the weight of our collective law enforcement and intelligence capabilities to bear against those who seek to do us harm.

We would be happy to answer any questions you have at this time.