



DEPARTMENT OF STATE

**WRITTEN STATEMENT
OF
EDWARD J. RAMOTOWSKI**

**ACTING ASSISTANT SECRETARY FOR VISA SERVICES
DEPARTMENT OF STATE**

**BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEE ON BORDER AND MARITIME SECURITY**

**HEARING
ON
TEN YEARS AFTER 9/11: CAN TERRORISTS STILL EXPLOIT OUR
VISA SYSTEM?**

SEPTEMBER 13, 2011

Good afternoon Madame Chairman Miller, Ranking Member Cuellar, and distinguished Members of the Committee. I thank you for this opportunity to update you on the steps we have taken to increase the security of the visa process.

The Department of State (the “Department”) is dedicated to the protection of our borders, and has no higher priority than the safety of our fellow citizens. We are the first line of defense in border security because the Department is often the first government agency to have contact with foreign nationals wishing to visit the United States. We are committed, along with our partner agencies, to a layered approach to border security that will enable the U.S. government to track and review the visa eligibility and status of foreign visitors from their visa applications throughout their travel to, sojourn in, and departure from, the United States.

Corrective Actions Implemented after December 25, 2009

After the December 25, 2009 attempted terrorist attack on Northwest Flight 253, the President ordered corrective steps to address identified weaknesses in the systems and procedures we use to protect the people of the United States. In the months following the attack, we reviewed our requirements for reporting potential terrorists who are not applying for visas, which fall under our “Visas Viper” program, as well as visa issuance and revocation criteria, and we introduced technological and procedural enhancements to facilitate and strengthen visa-related business processes.

Our immediate focus was on the deficiencies identified following the attempted attack on Flight 253 by Umar Farouk Abdulmutallab. On the day following his father’s November 2009 visit to the U.S. Embassy in Abuja, Nigeria, the Embassy sent a Visas Viper cable to the Department and the Washington intelligence and law enforcement community, stating that Abdulmutallab may be involved with Yemeni-based extremists. In sending the cable and checking State Department records to determine whether Abdulmutallab had a visa, Embassy officials misspelled his name, and as a result of that misspelling, information about previous visas issued to him, and the fact that he held a valid U.S. visa, was not included in the cable.

At the same time, the Consular Section entered Abdulmutallab’s name into the Consular Lookout and Support System (CLASS), our online database of lookout information. This correctly spelled CLASS lookout was shared automatically with the primary lookout system used by the Department of Homeland Security (DHS) and accessible to other agencies. On the basis of this CLASS entry, DHS’s U.S. Customs and Border Protection (CBP) determined, after the flight departed Amsterdam, that Abdulmutallab warranted secondary screening upon arrival in Detroit. Additional reporting on this case carried the correct spelling, with additional reports reaching the necessary agencies in Washington.

To address the deficiencies identified in that review, including our concerns with the Visas Viper process, we took immediate action to improve the procedures and content requirements for Visas Viper cable reporting. We directed all Chiefs of Mission to ensure that the Visas Viper program functioned effectively at their posts, and that all appropriate agencies and offices at post contributed relevant information for Viper nominations. We instructed consular officers to

include complete information about all previous and current U.S. visas in Visas Viper cables. The guidance cable included specific instructions on methods to comprehensively and intensively search the database of visa records so that all pertinent information is obtained. We also issued new instructions to officers regarding procedures and criteria used to revoke visas and reiterated guidance on consular officers' use of the discretionary authority to deny visas under section 214(b) of the Immigration and Nationality Act (INA), with specific reference to cases that raise security and other concerns. Instruction in appropriate use of this authority has been a fundamental part of officer training for several years.

In addition to changes in standard procedures for searching visa records, we immediately began working to refine the capability of our current systems, with a particular focus on matching records of currently valid visas against new and emerging derogatory information, to support visa revocation in appropriate cases. For visa applications, we employ strong, sophisticated name-searching algorithms to ensure matches between names of visa applicants and any derogatory information contained in the 42 million records found in CLASS. This robust searching capability, which takes into account variations in spelling, has been central to our procedures since automated lookout system checks were mandated following the 1993 World Trade Center bombing. We constantly use our significant and evolving experience with searching mechanisms for derogatory information to improve the systems for checking our visa issuance records.

CLASS has grown more than 400 percent since 2001 – largely as a result of improved data sharing among the Department, federal law enforcement agencies, and the intelligence community. Almost 70 percent of CLASS records come from other agencies, including information from the FBI, DHS, DEA and the intelligence community. CLASS also includes unclassified records regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the Terrorist Screening Center (TSC) and contains unclassified data on KSTs nominated by all U.S. government sources. We automatically run all applicants' names against the Department's Consular Consolidated Database (CCD), which holds our historical visa records, as part of our ongoing commitment to optimizing the use of our systems to detect and respond to derogatory information regarding visa applicants and visa holders. A system-specific version of the automated CLASS search algorithm runs the names of all visa applicants against the CCD to check for any prior visa applications, refusals, or issuances.

The Department has been continuously matching new threat information with our records of existing visas since 2002. We have long recognized this function as critical to the way we manage our records and processes. This system of continual vetting evolved as post-9/11 reforms were instituted, and is now performed in cooperation with the TSC. All records added to the Terrorist Screening Database are checked against the CCD to determine if there are matching visa records. Matches are sent electronically from the Department to TSC, where analysts review the hits and flag cases for possible visa revocation. In addition, we have widely disseminated our data to other agencies that may wish to learn whether a subject of interest has a U.S. visa.

Cases for revocation consideration are forwarded to the Department by our consular offices overseas, CBP's National Targeting Center (NTC), and other entities. As soon as information is established to support a revocation (i.e., information that could lead to an inadmissibility determination), a "VRVK" entry code showing the visa revocation is added to CLASS, as well as to biometric identity systems, and then shared in near-real time (within about 15 minutes) with the DHS lookout systems used for border screening. As part of its enhanced "Pre-Departure" initiative, CBP uses these VRVK records, among other lookout codes, to recommend that airlines should not board certain passengers on flights bound for the United States. Almost every day, we receive requests to review and, if warranted, revoke any outstanding visas for aliens for whom new derogatory information has been discovered since the visa was issued. Our Operations Center is staffed 24 hours a day, seven days a week, to address urgent requests, such as when a potentially dangerous person is about to board a plane. In those circumstances, the State Department can and does use its authority to revoke the visa, and thus prevent boarding.

The Department has broad and flexible authority to revoke visas and we use that authority widely to protect our borders. Since 2001, the Department has revoked approximately 60,000 visas for a variety of reasons, including nearly 5,000 for suspected links to terrorism; 1,451 of those occurring since the attempted attack on December 25, 2009. Following that incident, we reviewed the last ten years of Visas Viper nominations, as well as "P3B" entries (potentially ineligible for a visa due to suspected ties to terrorism) in CLASS to determine whether Visas Viper subjects were properly watchlisted, and to determine the visa status of all P3B subjects. The Department's Visa Office completed a review of all 2001-2010 data and revoked thirty visas.

Most revocations are based on new information that has come to light after visa issuance. Because individuals' circumstances change over time, and people who once posed no threat to the United States can become threats, revocation is an important tool. We use our authority to revoke a visa immediately in circumstances where we believe there is an immediate threat. At the same time, we believe it is important not to act unilaterally, but to coordinate expeditiously with our national security partners in order to avoid possibly disrupting important investigations.

A More Secure Visa Application Process

The Department constantly refines and updates the technology that supports the adjudication and production of U.S. visas. Under the Biometric Visa Program, before a visa is issued, the visa applicant's fingerprints are screened against DHS's Automated Biometric Identification System (IDENT), which has a watchlist containing available fingerprints of terrorists, wanted persons, and immigration law violators; and against the FBI's Integrated Automated Fingerprint Identification System (IAFIS), which contains more than 50 million criminal history records. More than 10,000 matches of visa applicants with records on the IDENT watchlist are returned to posts every month, normally resulting in visa refusals. In 2010, IAFIS returned more than 57,000 criminal arrest records to posts. The Biometric Visa Program partners with the DHS US-VISIT Program to enable CBP officers at ports of entry to match the fingerprints of persons entering the United States with the fingerprints that were taken during visa interviews at overseas posts and transmitted electronically to DHS IDENT. This biometric identity verification at ports

of entry has greatly enhanced CBP officers ability to identify photo-substituted visas and the use of valid visas by imposters.

We also use facial recognition technology to screen visa applicants against a watchlist of photos of known and suspected terrorists obtained from the FBI's TSC, as well as the entire gallery of visa applicant photos contained in our CCD. Facial recognition screening has proven to be another effective way to combat identity fraud.

The Consular Electronic Application Center (CEAC) is another major technological advance. CEAC is an electronic platform where applicants submit visa applications and photos via the Internet, eliminating paperwork, decreasing visa application and adjudication times, and reducing the number of forms applicants must complete. The worldwide rollout of the online DS-160 nonimmigrant visa application form is complete, and we are currently piloting the online DS-260 immigrant visa application form. These new online forms provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions, and soon will afford intelligence and law enforcement agencies opportunities to analyze visa application data before applicants appear for their interviews. The online forms offer foreign language support; however, applicants are required to answer in English, to facilitate information sharing between the Department and other government agencies. The new application forms are "smart," meaning that certain answers to questions will trigger subsequent questions. The system will not accept applications if the security-related questions have not been fully answered, and "irregular" answers are flagged to ensure that consular officers address them in the interview.

In April 2011, we greatly enhanced the way we track visa fraud. We globally deployed a tool called the Enterprise Case Assessment Service that provides a platform to store fraud-related research that used to be stored outside of consular systems. This new tool associates fraud-related information with visa records, making it available to consular officials around the world. Should fraud be confirmed during the course of a visa interview, consular officers can record that data in this new tool, where it can be easily referenced if the individual attempts to re-apply for a visa. Future iterations of this tool will track fraud in other consular services, such as U.S. passport applications, and will enable us to track the activities of third-party document vendors and visa fixers. We hope soon to be able to share this new data source with our U.S. government partners to enhance interagency cooperation on fraud prevention.

Student and Exchange Visitor Visas

I am aware that the members of this Committee have a keen interest in the processing of student and exchange visitor visas. Consular processing of these visa classes follows the same sequence of clearances as the other visa classifications, including collection of biometrics and submission of the on-line DS-160 form. All CLASS and other security checks apply.

In addition, in order for an applicant to demonstrate that he/she is qualified to apply for a student or exchange visitor visa, the applicant must have been issued specific documentation, in addition to what is required for other visas classes, and present it to the consular officer at the time of interview. A student, for instance, must have been issued a Form I-20A-B by the school he/she

will attend in order to apply for an F-1 student visa (or for dependants, an F-2 visa), or a Form I-20M-N if the student has been accepted at a vocational school. In order to qualify for an exchange visitor visa (J-1, dependent J-2), the applicant must present a Form DS-2019 issued by the designated sponsor of one of the 15 categories of exchange visitor programs.

Upon acceptance to the chosen educational institution or organization, the student or exchange visitor is assigned a unique ID number in the Student and Exchange Visitor Information System (SEVIS), a DHS database. The individual retains the same number throughout his or her educational career.

For an applicant to be found eligible for an F, M, or J visa, the student must meet the requirements specific to student or exchange visitor status (accepted at a school authorized by DHS to issue the Form I-20, pursuing a degree or certificate with sufficient finances, etc.) necessary to participate in the type of program chosen. In addition, the student must demonstrate the intent to engage only in approved activities for the visa class, the ability to meet the financial requirements of the activity undertaken, and demonstrate a present intent to depart the United States upon the completion of the chosen activity.

Training

Consular officers are trained to take all necessary steps during the course of making a decision on a visa application to protect the United States and its citizens. Every consular officer is required to complete the Department's Basic Consular Course at the National Foreign Affairs Training Center prior to performing consular duties. The course places strong emphasis on border security, featuring in-depth interviewing and name-checking technique training, as well as fraud prevention. Throughout their careers, consular officers receive continuing education in all of these disciplines to ensure they integrate the latest regulations and technologies into their adjudicatory decisions.

To augment this training and strengthen the security of the visa program, in early 2010 the Department launched a program to provide consular officers overseas with enhanced security clearances. This allows them to participate more fully in posts' review of security issues that bear on the issuance of passports and visas, and the protection of U.S. citizens traveling and living abroad. In the past few months, a concerted push on this project resulted in the tripling of the number of highly-cleared consular officers (to more than 150) in key positions at high threat posts. The Office of Counterintelligence and Consular Support, in the Bureau of Intelligence and Research, has increased its efforts to identify relevant reporting for review by those consular officers.

Security Advisory Opinions

The Department's Security Advisory Opinion (SAO) mechanism provides consular officers with the necessary advice and background information to adjudicate cases of visa applicants with possible terrorism ineligibilities. Consular officers receive extensive training on the SAO process, including modules on cultural and religious naming conventions, which assists them in identifying applicants who require additional Washington vetting. The SAO process requires the

consular officer to suspend visa processing pending interagency review of the case and additional guidance. Most SAOs are triggered by clear and objective circumstances, such as nationality, place of birth, residence, or visa name check results. In addition, in cases where reasonable grounds exist regardless of name check results, consular officers may suspend visa processing and institute SAO procedures if they suspect that an applicant may be inadmissible under the security provisions of the INA.

The Visa Security Program

The Department of State believes that the Visa Security Program (VSP), under which DHS deploys U.S. Immigration and Customs Enforcement (ICE) special agents to conduct visa security screening and investigations at certain overseas consular posts, is a valuable component of the U.S. government's overall policy of protecting our borders. We have a close and productive partnership with DHS, which has authority for visa policy under section 428 of the Homeland Security Act, and are fully supportive of the mission and future of the VSP, as well a number of data-sharing arrangements.

The VSP increases the utility of the visa application and interview processes to detect and combat terrorism, criminality, and other threats to the United States and the traveling public. ICE special agents assigned to Visa Security Units provide timely and valuable on-site vetting of visa applications and other law enforcement support to our consular officers. We work very closely with DHS to ensure that no terrorist receives a visa or is admitted into our country.

Reports from our posts with ICE visa security operations suggest that, as the VSP has matured over the past few years, ICE special agents have, where resources permit, moved beyond a singular focus on visa application review. They have been able to contribute their expertise and resources to enhance our response to all kinds of threats to the visa and immigration processes – terrorism, human smuggling and trafficking, and trafficking in a wide variety of contraband. As reported by one of our missions, “(i)n addition to their concerns with visa security, [ICE special agents’] efforts have also led to arrests and indictments in the areas of child pornography and countering the proliferation of controlled technology. This is a win-win partnership.”

In Washington, we work very closely with our VSP colleagues on day-to-day issues affecting the operations of the program, as well as longer term issues related to the expansion of the program to select overseas posts. VSP special agents in Washington review our visa databases and advise posts of emerging information about visa holders. Another important aspect of our Washington partnership is the resolution of issues raised as the VSP expands to more posts. In January 2011, the Department's Bureaus of Consular Affairs (CA) and Diplomatic Security (DS) concluded a Memorandum of Understanding (MOU) with ICE. This MOU governs VSP-Department of State interactions within visa sections, procedures for resolving the very few disputed visa cases that emerge from the VSP review process, and collaboration between ICE special agents and their DS law enforcement colleagues assigned as Regional Security Officers (RSOs) or Assistant Regional Security Officer Investigators (ARSO-Is) assigned to consular sections.

Under the umbrella of section 428 of the Homeland Security Act and the implementing Memorandum of Understanding between the Departments of State and Homeland Security, we work together to resolve cases. When warranted, DHS special agents assigned to the VSP will conduct targeted, in-depth reviews of individual visa applications and applicants prior to issuance, and recommend refusal or revocation of applications to consular officers. We work with DHS to ensure that terrorists do not receive visas and to expeditiously revoke visas as appropriate.

The Department works collaboratively with DHS, pursuant to an October 2004 MOU between the Department and the VSP on the “Administrative Aspects of Assigning Personnel Overseas,” and National Security Decision Directive 38 (NSDD-38). This directive outlines factors to be considered by Chiefs of Mission when considering requests by a U.S. government agency to create a new position at a post abroad. NSDD-38 gives Chiefs of Mission responsibility for the size, composition, and mandate of U.S. government agency staff under his or her authority.

Currently, there are 19 visa-issuing posts in 15 countries with an ICE VSP presence. Before submitting an NSDD-38 request, ICE officials, with the support of senior State Department officers from CA and DS, conduct a post-specific, on-site assessment. The visit provides an opportunity for the team to consult with officials at post to validate the interagency assessment of the risk environment, determine the feasibility and timing of establishing an office, and brief the Chief of Mission on the role of the VSP.

Layered Security and Data Sharing

The Department embraces a layered approach to security screening. In addition to our support of the VSP, over the past seven years the Department and DHS have increased resources significantly, improved procedures, and upgraded systems devoted to supporting the visa function. DHS receives all of the information collected by the Department during the visa process. DHS’s US-VISIT is often cited as a model in data sharing because the applicant information we provide, including fingerprint data, is checked at ports of entry to confirm the identity of travelers. DHS has broad access to our entire CCD, which contains more than 143 million records, related to both immigrant and nonimmigrant visas, covering the last 13 years. A menu of reports tailored to the specific needs of each particular unit is supplied to elements within DHS such as ICE’s agents assigned to conduct visa security investigations overseas.

We make all of our visa information available to other U.S. government agencies for law enforcement and counterterrorism purposes, and we specifically designed our systems to facilitate comprehensive data sharing with these entities. We give other agencies immediate access to more than 13 years of visa data for these purposes, and they use this access extensively. For example, in May 2011, over 23,000 officers from DHS, the Department of Defense (DoD), the FBI, DOJ, and the Department of Commerce submitted nearly two million queries on visa records in the course of conducting law enforcement and/or counterterrorism investigations.

Working in concert with DHS, we have proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the FBI, we have established the largest biometric screening program on the globe. We were a pioneer in

the use of facial recognition techniques and remain a leader in operational use of this technology. Currently, more than 146 million images are enrolled in our facial recognition database. In 2009, we expanded use of facial recognition from a selected segment of visa applications to all visa applications, and we are now expanding our use of this technology to passport records. We are testing use of iris recognition technology in visa screening, making use of both identity and derogatory information collected by DOD. These efforts require intense ongoing cooperation from other agencies. We have successfully forged and continue to foster partnerships that recognize the need to supply accurate and speedy screening in a 24/7 global environment. As we implement process and policy changes, we are always striving to add value in both border security and in operational results. Both dimensions are important in supporting the visa process.

In addition, every post that issues visas has a fraud prevention officer and locally employed staff devoted specifically to fraud prevention and document security. We have a large Fraud Prevention Programs office in Washington, which works closely with DS, and we have fraud screening operations using sophisticated database checks at both the Kentucky Consular Center in Williamsburg, Kentucky, and the National Visa Center in Portsmouth, New Hampshire. Their role in flagging questionable applications and applicants who lack credibility, present fraudulent documents, or give us false information adds a valuable dimension to our visa process.

DS adds an important law enforcement element to the Department's visa procedures. There are currently 75 ARSO-I positions approved for 73 consular sections overseas specifically devoted to maintaining the integrity of the process. In 2010, DS approved 48 additional ARSO-I positions to work in consular sections overseas. They are complemented by officers working domestically on both visa and passport fraud criminal investigations and analysis. These highly trained law enforcement professionals add another dimension to our border security efforts.

The multi-agency team effort, based upon broadly shared information, provides a solid foundation for securing our borders. The interagency community continues to automate processes to reduce the possibility of human error while at the same time enhancing our border security screening capabilities.

We face an evolving threat of terrorism against the United States. The people and the tools we use to address this threat must be sophisticated and agile and must take into account the cultural and political environment in which threats arise. Our officers must be well-trained, motivated, and knowledgeable. Information obtained from these tools must be comprehensive and accurate. Our criteria for taking action must be clear and coordinated. The team we use for this mission must be the best. The Department has spent years developing the tools and personnel needed to properly execute the visa function overseas and remains fully committed to fulfilling its essential role on the border security team.

Training Foreign Passport Officials

As part of our fraud prevention efforts, CA is working with the International Narcotics and Law Enforcement Affairs (INL) Bureau through INL's International Law Enforcement Academy (ILEA) network to provide passport antifraud training to officials from foreign passport issuance agencies.

The first class was piloted September 7-9, 2011 in El Salvador, for officials from various Central American countries. The training is designed to improve the integrity of other countries' passport issuance by helping them institute organizations, processes, and procedures for detecting fraudulent passport applications as part of their adjudication and issuance processes.

We plan to offer this training in 2012 at the ILEAs in Botswana and again in El Salvador.

Foreign Partner Capacity-Building Programs

The Department regularly engages our foreign partners bilaterally, regionally, and on a multilateral basis to address the issue of terrorist transit. This engagement involves a range of activities, including the exchange of information in a variety of security channels, the execution of capacity-building programs on border and document security, the provision of border screening programs like the Terrorist Interdiction Program/Personal Identification Secure Comparison and Evaluation System (TIP/PISCES), and regular consultations on broader issues.

Our capacity-building efforts are intended to foster regional cooperation and collaboration, whether through participation in organized regional groupings, such as the Trans-Sahara Counterterrorism Partnership, which facilitate regional training and exercises, or through assistance programs, such as the Regional Security Initiative (RSI), which funds regional Counterterrorism (CT) training and cooperative efforts across all CT priority regions.

The Department works in close coordination with the interagency community for the development and implementation of the full range of CT programming, through a range of fora. In addition to participation in regular National Security Council-led meetings, we have established mechanisms, such as the aforementioned RSI, which brings together our Embassy leadership with the full range of interagency representatives to discuss key issues of regional concern. This is replicated at the working level through the Regional Interagency Consultative Group. In North Africa, as already noted, we also have the Trans-Sahara Counterterrorism Partnership, through which State, DoD, and USAID cooperate and coordinate efforts to strengthen the counterterrorism capacity of our regional partners. The success of this approach has led to consideration of a similar construct for other regions. In addition to coordination through formal structures, we cooperate informally on a regular basis with the Departments of Defense, Justice, Homeland Security, and the Treasury on our counterterrorism efforts across the board.

U.S. Government Efforts to Stop Terrorist Travel

The U.S. government has many programs designed to thwart terrorist travel around the world. Many portions of the U.S. government play a critical role in stopping terrorist travel – DHS and its components, DoD, the law enforcement and intelligence communities, and State Department consular officers.

U.S. passports and visas contain sophisticated security features that make them very difficult to forge. The electronic chips in our passports and the machine readable lines on our visas employ some of the most sophisticated technical security measures available. State Department consular

officers work with our partners from CBP and ICE to train foreign border and airline personnel in the detection of fraudulent travel documents. The Department's Office of the Coordinator for Counterterrorism (S/CT) also helps foreign partners at risk for terrorist activity to establish their own computerized stop-list systems via the TIP/PISCES program.

In the additionally critical areas of international travel document security and interoperability, we have intensified our work. With passport-issuing authorities of International Civil Aviation Organization (ICAO) member States around the globe, we have striven to ensure that, as with the U.S. ePassport, other issuing authorities meet internationally established standards for security and interoperability. This has included the cooperative and growing use of the Public Key Directory (PKD), which is centrally managed and overseen by a board of actively participating ICAO member states. The PKD is a directory used by a receiving state to verify the digital signature used by a travel document's issuing authority, thereby authenticating the passport in real time.

The ePassports, which we have been issuing since December 2005, introduce a new class of security feature to identity documents: a digital signature. The validation of a signature guarantees that the chip contents, which include the facial image, are genuine and belong to the physical document. Only on this basis can it be proven that a specific ePassport was issued to the person that claims to be the rightful owner. The ICAO PKD is integral to the effort to have an efficient and commonly accepted means of sharing and updating digital signatures (public keys) used by the world's ePassport-issuing authorities.

Where validation using the ICAO PKD occurs during travel, whether at points of embarkation, transit, or upon entry, it provides much greater levels of assurance than are currently possible with traditional machine readable travel documents. Border inspectors will be better able to identify inadequately documented travelers. Border inspectors worldwide can, in effect, assist the issuing authority in enhancing the integrity of all ePassports.

The benefits of the ICAO PKD increase exponentially as the number of States participating, and the number of ePassports in circulation, increase. Participating States and entities stand to benefit most, because their participation in the ICAO PKD maximizes global coverage of validation of their travel documents.

Electronically reading the PKI adds a third level of security for biometric passports, joining visual/tactile and laboratory features of the document, and scanner reading of the biometric content. This combination of features constitutes a tool bag for CBP officers to use in verifying the authenticity of the person and his/her passport when entering the United States.

The U.S. government's advanced information-sharing initiatives ensure that we and our international partners are in constant contact regarding the threat of terrorist travel. CBP's use of Advance Passenger Information (API) and Passenger Name Record (PNR) data are valuable tools in detecting travel patterns and co-travelers of terrorist suspects. The U.S. government's agreements with foreign partners under Homeland Security Presidential Directive (HSPD) 6 allow us to share terrorist screening information with trusted partners, in order to interdict known and suspected terrorists.

We also have entered into arrangements for the sharing of visa information with foreign governments, consistent with the requirements of section 222(f) of the INA. Since 2003, there have been arrangements in place with Canada for such sharing under certain circumstances. With DHS, the Department is participating in a pilot program, through the Five Country Conference (United States, Australia, Canada, New Zealand, and the United Kingdom) for identification of travelers based on biometric matching in some individual cases. We are in negotiation with the governments of Canada and the United Kingdom for agreements that would provide a legal basis for us to implement arrangements for the automated sharing of visa refusal data and for systematic confirmation of an applicant's identity through biometric matching. These arrangements would be limited to information regarding nationals of third countries. We expect both agreements to be completed this year, and similar agreements with Australia and New Zealand in 2012.

The Department plays a key role in all of these international initiatives. With our partners at the TSC, we negotiate the HSPD-6 agreements overseas. We are a close partner with DHS in API and PNR discussions overseas, in particular with respect to the current talks with the European Union on PNR. Together, all of these programs are helping achieve the goal of constraining terrorist mobility. This is our obligation to the American people.

Conclusion

We believe that U.S. interests in legitimate travel, trade promotion, and educational exchange are not in conflict with our border security agenda and, in fact, further that agenda in the long term. Our long-term interests are served by continuing the flow of commerce and ideas that are the foundations of prosperity and security. Acquainting people with American culture and perspectives remains the surest way to reduce misperceptions about the United States. Fostering academic and professional exchanges keeps our universities and research institutions at the forefront of scientific and technological change. We believe the United States must meet both goals to guarantee our long-term security.

Our global presence, foreign policy mission, and personnel structure give us singular advantages in executing the visa function throughout the world. Our authorities and responsibilities enable us to provide a global perspective to the visa process and its impact on U.S. national interests. The issuance and refusal of visas has a direct impact on our foreign relations. Visa policy quickly can become a significant bilateral problem that harms broader U.S. interests if handled without consideration for foreign policy equities. The conduct of U.S. visa policy has a direct and significant impact on the treatment of U.S. citizens abroad. The Department of State is in a position to anticipate and weigh all those factors, while ensuring border security as our first priority.

The Department has developed and implemented an intensive visa application and screening process requiring personal interviews, employing analytic interview techniques, incorporating multiple biographic and biometric checks, all supported by a sophisticated global information technology network. We have visa offices in virtually every country of the world, staffed by consular officers drawn from the Department's professional, mobile, and multilingual cadre of

Foreign Service Officers. These officials are dedicated to a career of worldwide service, and provide the cultural awareness, knowledge, and objectivity to ensure that the visa function remains the frontline of border security. Each officer's experience and individual skill set are enhanced by an overall understanding of the political, legal, economic, and cultural development of foreign countries in a way that gives the Department of State a special expertise over matters directly relevant to the full range of visa ineligibilities.

This concludes my testimony today. I will be pleased to take your questions.

