DEPARTMENT OF STATE

WRITTEN STATEMENT

OF

JANICE L. JACOBS

ASSISTANT SECRETARY OF STATE FOR CONSULAR AFFAIRS

DEPARTMENT OF STATE

BEFORE THE

UNITED STATES SENATE

COMMITTEE ON HOMELAND SECURITY AND

GOVERNMENTAL AFFAIRS

HEARING

ON

TEN YEARS AFTER 9/11: PREVENTING TERRORIST TRAVEL

JULY 13, 2011

Good afternoon, Chairman Lieberman, Senator Collins, and distinguished Members of the Committee. This is my third appearance before your committee on this important topic and I thank you for the opportunity to update you on the steps we have taken to increase the security of the visa process. I am also joined by my colleagues from the Bureau of Population, Refugees and Migration (PRM) and the Office of the Coordinator for Counterterrorism, who are here to answer your questions on these topics.

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, with our partner agencies, to a layered approach to border security that will afford us the ability to track and review the visa eligibility and status of foreign visitors from the time they first apply for a visa and throughout their travel to, sojourn in, and departure from the United States.

Corrective Actions Implemented after December 25, 2009

After the December 25th, 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 "Visas Viper" requirements for reporting potential terrorists, as well as related visa issuance and revocation criteria, and 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 same file in Washington.

After reviewing these events, 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 was working 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 search comprehensively and intensively the database of visa records so that all pertinent information is obtained. We also issued new instructions to officers regarding procedures and criteria used in the field 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 39 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 use our significant and evolving experience with searching mechanisms for derogatory information to improve the systems for checking our visa issuance records constantly.

CLASS has grown more than 400 percent since 2001 – largely the result of improved sharing of data 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 intelligence from other agencies. CLASS also includes derogatory information regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the Terrorist Screening Center (TSC) and contains the 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 all our 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 by the TSC. All records added to the Terrorist Screening Database are checked against CCD to determine if there are matching visa records. Matches are sent electronically from the TSC to the Department of State to 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 us by our consular offices overseas, CBP's National Targeting Center (NTC), and other entities. As soon as information is established to support a revocation, 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 (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 to airlines that certain passengers should not be boarded on flights bound for the United States. Almost every day, we receive requests to review and, if warranted, revoke visas for potential travelers 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 prudentially, 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 nearly 60,000 visas for a variety of reasons, including 4,000 for suspected links to terrorism; 1,320 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 prudentially revoked thirty visas.

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 consultation

with national security partners is critical. Expeditious coordination with our national security partners is not to be underestimated. Unilateral and uncoordinated revocation could disrupt important investigations undertaken by one of our national security partners.

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 contains 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. 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; more than 10,000 hits are returned to posts every month from IDENT. (Not all IDENT hits result in visa refusals. For example, some records refer to deportations or voluntary removals that occurred up to twenty years ago, among other records that do not constitute any statutory ineligibility.) This biometric identity verification at ports of entry ensures the security of the U.S. visa by essentially eliminating the possibility of visa fraud through counterfeit or photo-substituted visas, or through the use of valid visas by impostors.

We also use facial recognition technology to screen visa applicants against a watch list of photos of known and suspected terrorists obtained from the FBI's Terrorist Screening Center (TSC), as well as against the entire cache 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 to one 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. They also 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, but 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 subsequent questions are triggered by an applicant's answers to earlier 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 officers address them in the interview.

In April 2011, we greatly enhanced the way we track visa fraud. We deployed globally a tool called the Enterprise Case Assessment Service that provides a

platform to store fraud-related research that used to be stored, for the most part, 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. 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 are exploring the possibility of sharing this new data source with our U.S. government partners to enhance interagency cooperation on fraud prevention.

Training

Consular officers are trained to take all necessary steps to protect the United States and its citizens during the course of making a decision on a visa application. Each 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.

Security Advisory Opinions

In addition, the Department's Security Advisory Opinion (SAO) mechanism provides 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 cultural and religious naming conventions, which assists them in identifying applicants requiring 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, to suspect that an applicant may be inadmissible under the security provisions of the INA, consular officers suspend processing and institute SAO procedures.

Consular officers refused approximately 23 percent of nonimmigrant and immigrant visas in FY 2010 (2,170,154 applications out of a total of 9,074,958 applications). The results of these checks by consular officers and any fraud indicators are brought to the attention of DHS's Visa Security Units and/or consular fraud officers wherever they are posted abroad.

The Visa Security Program

The Department of State believes that the Visa Security Program (VSP) 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 maximizes 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. U.S. Immigration and Customs Enforcement (ICE) special agents assigned to Visa Security Units (VSUs) 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 VSU posts suggest that, as the VSP has matured over the past few years, VSU personnel have, where resources permit, moved beyond a singular focus on visa application review, and 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 human 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, [VSU 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 officers 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 that are 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 VSU-Department of State interactions within visa sections, procedures for

resolving the very few disputed visa cases that emerge from the VSU review process, and collaboration between ICE/VSU 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 corresponding Memorandum of Understanding between the Departments of State and Homeland Security, we work together to resolve cases. When warranted, DHS officers assigned to VSUs 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 ICE/VSP on the Administrative Aspects of Assigning Personnel Overseas, and National Security Decision Directive 38 (NSDD-38). This directive outlines factors to be considered when deciding whether establishing a VSU is appropriate at a particular post. 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, 19 VSUs are active at posts in 15 countries. 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 COM on the role of the VSU.

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 information we share on applicants, 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 over 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 VSUs.

We make all of our visa information available to other agencies, and we specifically designed our systems to facilitate comprehensive data sharing. We give other agencies immediate access to over 13 years of visa data, and they use this access extensively. For example, in May 2011, almost 22,000 officers from DHS, the Department of Defense (DoD), the FBI, DOJ, and the Department of Commerce submitted nearly two million queries on visa records.

Working in concert with DHS, we proactively expanded biometric screening programs and integrated this expansion into existing overseas facilities. In partnership with DHS and the FBI, we 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, over 142 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 beyond visa 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 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, we have 145 officers and 540 locally employed staff devoted specifically to fraud prevention and document security, including fraud prevention officers at overseas posts. We have a large Fraud Prevention Programs office in Washington, which works very 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 on border security, based upon broadly shared information, provides a solid foundation. At the same time we remain fully committed to correcting mistakes and remedying deficiencies that inhibit the full and timely sharing of information. We have, and will continue to automate processes to reduce the possibility of human error. We are working and will continue to work to continually enhance our border security screening capabilities, and the contributions we make to the interagency effort.

We are facing an evolving threat. 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. The people 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 continuing to fulfill its essential role on the border security team.

Special Immigrant Visas for Iraqis

I am aware that the members of this Committee have a keen interest in Iraqi nationals working on behalf of the U.S. government in Iraq, who come to this

country as recipients of special immigrant visas (SIVs) or as refugees. More specifically, I know of your concern for the security of the process that brings them here. Following the recent arrest for terrorism activities of two Iraqis who arrived in the United States under the Iraqi refugee program, we are making special efforts to ensure the security of the SIV program as well as the refugee program.

The United States recognizes a special responsibility to Iraqis with U.S. affiliations and has developed several programs that can facilitate their access to resettlement in the United States. There are two categories of SIVs for Iraqis working for or on behalf of the U.S. government in Iraq. As of June 11, 2011, a total of 7,063 Iraqis have been issued special immigrant visas under the following two SIV programs – 1,629 Iraqis have been issued an SIV under the program established in section 1059 of the National Defense Authorization Act of 2006 for translators and interpreters, and 5,434 Iraqis have been issued a SIV under the program established in section 1244 of the National Defense Authorization Act of 2008 for other types of employment.

Many Iraqis who are eligible for a SIV opt to apply for the separate U.S. refugee resettlement program instead. As of June 22, 2011, over 59,000 Iraqi refugees have been resettled in the United States since 2007. We use 2007 as a starting point because Iraqis were not fleeing in large numbers until 2006, when the sectarian violence began in response to the bombing of the mosque in Samara. Under the law, an Iraqi applicant's spouse and minor children are also eligible for SIVs. Because some extended family members may be eligible under the refugee program, under exceptional circumstances, but not under the SIV program, the refugee resettlement program may be preferred by those who want their extended family to resettle together at the same time.

We make every effort to streamline the SIV process where possible, while ensuring that Iraqi refugees and recipients of SIVs – like all of those who enter the United States – do not pose a threat to the security of the United States. However, implementing some of our newer security procedures has limited our progress in streamlining the SIV application process.

The Department is committed to issuing SIVs only to those qualified for the program. While we cannot discuss specifics for security reasons, SIV applicants from Iraq as well as Afghanistan undergo multiple layers of review. Over the past six months, we have worked with DHS and others to enhance the security screening process further to address potential security threats. In the past year, the Department of State, working with DoD and DHS, has continued to adjust our SIV application procedures to cut months off our processing times. We no longer require documentation that we found to be redundant; we have decreased the amount of paperwork that must be submitted by mail in favor of electronic submissions; and we have reorganized internal procedures so that the process moves faster. We are in the process of implementing additional improvements to be launched in the coming months.

Securing Refugee Admissions

In addition to its responsibility for the efficacy and security of the visa process, the Department is also responsible for the management of major parts of the U.S. Refugee Admissions Program, along with DHS and other U.S. federal and state agencies and offices.

Every year, the United States admits tens of thousands of refugees as part of a humanitarian effort that reflects the highest values and aspirations of the American people, in a program that is authorized by Congress and historically has enjoyed broad bipartisan Congressional support. For decades, American communities have opened their hearts, homes, and neighborhoods to refugees from around the world. Our responsibility is to ensure that they do so with continued confidence in the security of the program.

Specifically, the Department's PRM Bureau, through its Resettlement Support Centers, conducts preliminary overseas pre-screening of refugee applicants for U.S. admissions, collecting pertinent biographic information necessary for numerous consular, law enforcement, and intelligence reviews. All refugee applicants for U.S. admissions are subject to the CLASS check and certain refugee applicants undergo the SAO check – both of which were discussed earlier in this testimony. DHS, which has final adjudicative authority for refugee admissions to the United States, coordinates numerous additional law enforcement and intelligence checks before granting admission to a refugee and his or her family.

The Department and DHS have taken a number of steps in recent years to strengthen the security screening of refugees, including through expanded intelligence community participation and elevated screening for certain refugee populations. We will continue to look for additional ways to enhance the security of this important humanitarian program.

Training Foreign Passport Officials

As part of our fraud prevention efforts, Consular Affairs 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 will be piloted in September 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.

CA plans to offer this training at the ILEAs in Botswana and again in El Salvador in 2012.

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 through regular consultations on broader issues like we have with the EU and other capable partners. 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, which funds regional 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 counterterrorism 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 Regional Security Initiative (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 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, 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. 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 International Civil Aviation Organization (ICAO) member passport-issuing authorities around the globe, we have strived to ensure that, as with the U.S. passport, other issuing authorities meet internationally established standards for security and interoperability. This has included the cooperative and growing use of the Public Key Infrastructure (PKI), which is centrally managed and overseen by a board of ICAO member states that are active participants. Electronically reading the PKI, which assures the country name on the passport is the same country that issued the document, 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 advance 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 State 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 next year.

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 exchange 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.

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 present 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 is 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.