DEPARTMENT OF STATE

STATEMENT
OF

AMBASSADOR JANICE L. JACOBS

ASSISTANT SECRETARY OF STATE FOR CONSULAR AFFAIRS,
BUREAU OF CONSULAR AFFAIRS,
DEPARTMENT OF STATE

BEFORE THE
SENATE COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

HEARING
ON
FIVE YEARS AFTER THE INTELLIGENCE REFORM AND TERRORISM ACT: STOPPING TERRORIST TRAVEL

DECEMBER 9, 2009

Chairman Lieberman, Ranking Member Collins, and distinguished Members of the Committee, it is a distinct honor to appear before you today. I would like to express my sincere appreciation for the opportunity to share with you many of the accomplishments of my colleagues in the Bureau of Consular Affairs (CA) in our continuing efforts to strengthen the security of U.S. borders through the vigilant adjudication of U.S. passports and visas while maintaining America's traditional openness to legitimate travelers.

Introduction

Defending security at the borders of the United States starts with consular officers overseas. CA's visa adjudication function and prevention of fraudulent use of U.S. travel documents are one of our first lines of defense against terrorists and others who would do us harm. U.S. visas and passports are some of the most coveted travel documents in the world. We place the utmost importance on the integrity of our visa and passport issuance processes to ensure that only those who meet the eligibility requirements for U.S. travel documents receive them. Our close and fruitful cooperation with our closest partner agencies – the Department of Homeland Security (DHS) and the Justice Department's FBI – supports and strengthens these missions.

Executive Summary

The following is a summary of the technological, procedural, data-sharing, interagency cooperation, training and other enhancements CA has implemented since September 11, 2001 and the enactment of the Intelligence Reform and Terrorism Act. If we were to take a snapshot of our consular activities in August of 2001 and compare it with a snapshot of our operations today, you would see dramatic improvements. In 2001, the Consular Lookout and Support System (CLASS), the database the Department uses to check visa and passport applicants for derogatory information, contained approximately seven million visa records and 2.2 million passport records. At that time CLASS connectivity with Washington could be lost for extended periods, and officers would be forced to use a back-up system – a CD-ROM replica of the database that could have been a month old. In 2001, consular officers depended largely on information provided by the visa applicants to determine their identities. If a visa applicant turned out to be a possible match for a terrorism-related CLASS record, the consular officer requested a Security Advisory Opinion (SAO) from the Visa Office in Washington. Such requests were sent via cables, as were the Department's responses. This multi-step cable process to communicate with posts and to coordinate with other government agencies resulted in long wait times for both the consular officers and the applicants.

Since September 11, 2001, we have revamped our procedures and introduced new technology that makes adjudicating visa and passport applications both more efficient and effective. Barriers to the exchange of information have come down throughout the U.S. government (USG). The CLASS database has grown more than more than 400 percent, to 26 million records, and grown more robust. Improvement in real time connectivity has put an end to CD-ROM back-up systems. This increase in the quantity and quality of CLASS records is largely the result of improved data sharing between the Department of State and the law enforcement and intelligence communities. In 2001, only 25 percent of records in CLASS came from other government agencies. Now, almost 70 percent of CLASS records come from other agencies. The use of biometrics has become standard in the visa process. Using fingerprints and facial recognition technology, we can fix identities through biometric enrollment and biometrically match applicants to derogatory information.

One of the most far-reaching technological improvements in visa operations was the development of the Consular Consolidated Database (CCD). The CCD is a powerful, integrated tool that allows Foreign Service posts, the Department, and our partner agencies and offices to view information about visa applicants. To the extent such access is permitted under confidentiality provisions of the Immigration

and Nationality Act, such information includes photographs, facial recognition check results, comments made by interviewing officers, CLASS namechecks, DHS's Automated Biometric Identification System (IDENT) and FBI's Integrated Automated Fingerprint Identification System (IAFIS) results, and supporting documents. At present, the CCD has more users from other government agencies than from our Department.

The SAO process, by which select visa applicants are screened and cleared by other government agencies prior to visa issuance, has undergone major enhancements. We have done away with cable communications for SAO requests and established direct electronic connectivity between overseas consular posts and Washington agencies. This connectivity allows the government agencies responding to SAO inquires to use the same visa systems that posts use overseas. This direct linkage between the Department and our partner agencies facilitated the Visa Office's processing of nearly two million SAO requests since September 11, 2001. Since that date, we and our partner agencies have engaged in a nearly constant round of SAO process refinements and resource allocations. One result of our dedication to this effort is that, at this time, we have the shortest SAO turnaround times since September 11, 2001 – maintaining the security of our borders while reducing the impact on legitimate travelers.

The wide range of technologies now available to assist consular officers in gathering, organizing and sharing information relevant to visa applications is paralleled by advances in consular training. New consular officers benefit from an increased focus on the security-related aspects of visa adjudication. A continuum of courses covering fraud prevention, interviewing, namechecking, management, and more are offered at the Foreign Service Institute (FSI) in Arlington, Virginia, as well as online training resources available at posts. FSI continuously works with offices throughout the government to develop new training opportunities that meet the challenges of the changing world in which consular officers operate.

Visa and Passport Processing Today

Technology and the Visa Process

The Department of State constantly refines and updates the technology that supports the adjudication and production of U.S. visas. There are many examples of how enhancing the security of the document directly improves the security of U.S. borders. Under the Biometric Visa Program, before a visa is issued, the visa applicant's fingerprints are screened against IDENT, which contains all available fingerprints of terrorists, wanted persons, and immigration law violators, and against IAFIS, which contains more than 50 million criminal history records. The

Biometric Visa Program partners with the DHS US-VISIT Program to enable Customs and Border Protection (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 post and transmitted electronically to DHS IDENT. 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 imposters.

In 2007, we transitioned from capturing two fingerprints at the time of visa adjudication to taking all ten prints. In FY 2009, fingerprints of more than 6.7 million visa applicants were screened against IDENT and IAFIS databases. From IAFIS, more than 49,000 criminal arrest records were sent to posts. More than 10,000 watch list hits are returned to posts every month from IDENT.

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 identify fraud.

Today, every visa applicant undergoes extensive security checks before a visa can be issued. The CLASS namecheck system, which is updated daily, includes information from the Department of State, FBI, DHS, and intelligence from other agencies. Also included in CLASS is derogatory information regarding known or suspected terrorists (KSTs) from the Terrorist Screening Database, which is maintained by the TSC and contains the names of terrorists nominated by all USG sources. Possible matches are reviewed by USG agencies in Washington, D.C., prior to any visa being issued. Under a complementary program, new name entries in the Terrorist Screening Database are checked against records of previously issued valid visas, enabling us to revoke visas issued to KSTs. Since September 11, 2001, we have revoked more than 1,700 visas of individuals about whom, subsequent to visa issuance, we received information that potentially connected the visa holder to terrorism.

In October 2008, the Department of State took over responsibility for producing the Border Crossing Card (BCC) used as a visa by Mexican nationals to cross the southern border. The Department of State extensively redesigned the BCC, and made it compatible with the radio frequency (RFID) technology used by CBP at land ports of entry. The RFID chip on the card contains a number that allows the CBP system to access the card issuance data forwarded by the Department of State

to a secure DHS database. The card issuance data, including the bearer's photo, appears on the computer screen of the CBP officer when a vehicle arrives at the primary inspection booth. This new BCC facilitates both the inspection process for the CBP officers and the entry process for qualified Mexican nationals entering the United States.

Another major technological advance is the Consular Electronic Application Center – a new 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. This new online system, now being deployed overseas, will provide consular and fraud officers the opportunity to analyze data in advance of the interview, enhancing their ability to make decisions. The online form offers foreign language support, but applicants will be required to answer in English, to facilitate information sharing between the Department of State offices 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 make note of them.

The Consular Visa Interview

One of the most significant changes in consular practice after September 11, 2001, was a re-emphasis on the personal interview. Requirements for in-person interviews of visa applicants were codified in the Intelligence Reform and Terrorism Prevention Act. The interview is an opportunity for consular officers to assess the credibility of the applicant and the applicant's travel plans. Consular officers are trained in interview techniques, foreign languages, and cultural awareness skills they leverage during visa interviews. Because misrepresentation or fraud can be present in a variety of forms, such as false documents, fictitious relationships and identities, and mutilated fingerprints, CA employs a layered approach to secure the integrity of the visa adjudication process. We have put in place an array of measures, including analytic interviewing techniques, biometric checks, database checks, and document verification. This layered approach poses a significant obstacle and deterrent to foreign persons seeking entry to the United States to do us harm.

Fraud Prevention Techniques

We have a variety of tools available, in addition to the consular interview, to separate fact from fiction in visa applications. Since 2001, we have increased the

number of staff dedicated to the prevention of consular fraud. Consular fraud prevention personnel posted domestically and abroad have developed robust networks and mechanisms to verify information presented in visa applications. We employ increasingly sophisticated tools to detect links between different fraudulent cases and analyze fraud trends.

CA will also soon deploy a global system called the Consular Case Management Service (CCMS) for tracking and conducting consular fraud investigations. This system, among other things, will improve consular officers' ability to easily and effectively share information on suspect cases. We expect to release the first phase of the system, which will support the full spectrum of visa fraud cases, to posts worldwide in early 2010. Future deployments will add the capability to manage passport fraud cases – both overseas and domestically. We believe CCMS will greatly enhance our ability to track and analyze global fraud trends.

Inter-departmental Cooperation

Our principal goals in visa adjudication are to facilitate travel that is legitimate and prevent travel that is not. Often, however, we run across cases involving organized crime or fraud that may be prosecutable in the United States or under local law. In such instances we turn immediately to our law enforcement colleagues in the

Bureau of Diplomatic Security (DS). CA and DS coordinate very closely. Many DS agents go through the Basic Consular Course, the same one all consular officers take as part of their initial training, and may be assigned as overseas criminal investigators based in consular sections abroad. In many cases, based on DS's excellent liaison relationships with local police, a perpetrator of fraud not only is denied a visa, but is then placed under arrest at the front gate on departing the embassy. In some cases, information gathered as a result of these investigations overseas is also used to disrupt and prosecute sophisticated document fraud operations in the United States. This coordination with DS is a very powerful factor in deterring terrorists' attempts to secure visas, as well as deterring other kinds of fraud.

CA and DS have established a jointly-staffed Consular Integrity Division (CID) within CA's Office of Fraud Prevention Programs. The CID is responsible for strengthening internal controls throughout CA and investigating cases of internal corruption or malfeasance, for which we adhere strictly to a policy of zero tolerance.

In July 2007, a Government Accountability Office (GAO) Report on border security recommended developing close coordination and liaison among

counterfeit deterrent specialists within DHS and other Federal agencies. CA continues to develop this capacity, including the creation this year of the Forensic Document Design and Integrity Coordination function. This coordinating mechanism draws together a team of professionals from all areas of CA who are committed to "state of the art" counterfeit document deterrence. Their recommendations have already brought about improvements in security documents.

Visa Waiver Program

Not everyone requires a visa to travel to the United States. We have worked closely with DHS to increase the security of the Visa Waiver Program (VWP). Together with DHS's Visa Waiver Program Office, we are engaging VWP member countries to help them meet the enhanced security requirements contained in the *Implementing Recommendations of the 9/11 Commission Act of 2007 (the 9/11 Act)*. CA also worked closely with DHS's CBP on the creation of the Electronic System for Travel Authorization (ESTA) and continues to assist in its implementation. In fact, ESTA provides a lookout to our CLASS system for every ESTA authorization DHS denies, thereby informing consular officers when a visa applicant had previously attempted to obtain an ESTA approval. ESTA also uses visa refusal records from CA to check applications against.

Technology and the Passport Process

Recognizing that the U.S. passport is one of the most sought-after travel documents in the world, CA has committed itself to issuing passport documents that include advanced technological features to foil the efforts of counterfeiters. We are also doing everything in our power to ensure that passports are issued only to U.S. citizens who are eligible to receive them.

In August 2006, the Department of State began issuing the ePassport, the first U.S. passport to contain a contactless chip that stores the bearer's photograph and biographical data. The data is secured through the use of public key cryptography and digital signatures. This is a transformational step forward in document security. Unlike paper passports, where a photo could be potentially substituted or the biographic data overwritten, the information on the chip, once locked by the key, cannot be changed. There are more than 45 million U.S. ePassports in use.

In July 2008, to address one of the key objectives of the Western Hemisphere Travel Initiative, we began issuing a passport card. The passport card is a driver's license-sized card that contains a contactless chip. No personal information is contained in the chip – only a unique number that, once read, points to the bearer's

information in secure DHS databases. The passport card uses state-of-the-art security features to prevent counterfeiting and forgery.

As important as the security of documents themselves is the integrity of the passport adjudication process, including the electronic databases used to screen passport applicants and verify their citizenship and identity. All valid U.S. passports are supported by the Passport Information Electronic Records System (PIERS), a database of more than 214 million passport records, including photos, applications, and history. PIERS is available to consular officers and passport adjudicators worldwide to verify the identity and citizenship of those to whom U.S. passports have previously been issued. We have granted access to PIERS data to several components of DHS, law enforcement and intelligence agencies to aid in successfully protecting our borders. With each of these agencies, we also have agreements in place to ensure that the proper training, monitoring, and reporting procedures are in place to safeguard the personally identifiable information of every passport applicant.

The Consular Lost and Stolen Passports (CLASP) database includes more than eight million records concerning U.S. passports. CLASP data is shared with DHS and other domestic law enforcement and intelligence agencies as well as with

international organizations such as Interpol. In addition, the Department of State maintains 24/7 operations to help foreign authorities check on U.S. passport validity and authenticity, using the CLASP database.

All domestic passport applications are checked against CLASP, PIERS, the Social Security Administration's (SSA) database, and CLASS, which includes, among other data, information provided by the Department of Health and Human Services and federal, state, and local law enforcement agencies. CA is holding discussions with SSA to obtain real-time access to their data to conduct verifications.

Recent evaluations of our passport adjudication process by the GAO and the Department of State's Office of the Inspector General identified areas of vulnerability. In response, we have greatly enhanced our fraud-prevention efforts over the past year. In coordination with DS, we launched a program that consists of unannounced testing of the processes and procedures for passport acceptance and adjudication in much the same manner used by the GAO. The program is an ongoing effort to test systematically for potential individual and systematic vulnerabilities. Each test scenario will be followed by on-site training for employees of the affected passport agency and/or acceptance facility, and immediate reporting to CA of any deficiencies in our systems or procedures. We

expect to correlate lessons learned, facilitate debriefing and training to employees and management, provide constructive suggestions on systematic improvements to mitigate these vulnerabilities, and strengthen management controls.

We have also reached out to interagency law enforcement and state government partners to enhance our ability to detect fraudulent documents such as birth certificates and driver's licenses submitted to support citizenship and identity in passport applications.

Data Sharing

Distinguished Members of the Committee, cooperation with partner USG agencies and departments is the critical foundation of our mission. In accordance with both the Department of State's own objectives of detecting and stopping would-be terrorists and the provisions of the Enhanced Border Security and Visa Entry Reform Act of 2002, we have taken significant steps to increase the quantity and efficiency of data sharing between the Department of State and the law enforcement and intelligence communities.

In one recent month, more than 12,000 employees at other agencies and entities including DHS, the FBI, the Department of Defense, TSC, the National

Counterterrorism Center, and the Department of Commerce submitted 900,000 queries on visa records to the CCD, which, as noted previously, includes information such as photos of visa applicants, consular officer notes on visa cases, and relevant documents scanned into the database. CA also has data sharing agreements with these same agencies to access passport records for known or suspected persons of interest.

Visa applicant data, including photographs, is replicated within minutes from posts worldwide to the CCD, which relays it to the DHS TECS computer system for use by CBP officers at ports of entry. This rapid visa data sharing allows visa records, including photos, to be displayed on CBP officers' computer screens as travelers present their visas at ports of entry. Department of State also provides U.S. passport issuance data, including photographs, to the DHS TECS computer system for use by CBP officers to verify U.S. passports the same way they verify visas. Certain DHS officers can also access passport data in PIERS, ensuring the ability to verify U.S. citizen identities at ports of entry.

We increasingly rely on data from our partners to enhance our ability to make the right decisions when adjudicating visa and passport applications. A valuable tool to which we have recently been granted access is DHS's Arrival Departure

Information System (ADIS). ADIS tracks foreign nationals' entries into and most exits out of the United States. The tool has uncovered previously undetected cases of illegal overstays in the United States that render foreign nationals ineligible for visas. ADIS is currently available to a limited number of consular officers, but DHS and CA are working together to make entry-exit data broadly available to all interviewing consular officers by March 2010.

CA and DHS are also working to provide consular officers access to several other DHS systems, especially those that U.S. Citizenship and Immigration Services (USCIS) use to adjudicate immigration and naturalization benefits within the United States. We are also pursuing access to various other DHS databases that would assist us in pre-screening visa applicants before they appear for their interviews.

The State Department and the TSC have also concluded formal agreements or arrangements with 17 foreign partners for the reciprocal exchange of terrorism screening information, which enhance our existing channels of information sharing about known and suspected terrorists. Thirteen of these countries are Visa Waiver Program countries. We continue to work with the TSC to expand these bilateral cooperative arrangements.

As I mentioned, we already have a data sharing relationship with the SSA that allows us to check passport applications against their databases to ensure that passport applicants are not using the identities of deceased U.S. citizens. We have an agreement in place with the National Association for Public Health Statistics and Information Systems to facilitate verification of birth certificates presented in support of passport applications. The association has provided us with access to the Electronic Verification of Vital Events (EVVE) system, which allows CA to verify vital records' data from 17 states. All 50 states are expected to participate in EVVE by 2011. This tool is currently available to our fraud prevention offices and we are looking to expand its use to passport adjudicators in the near future.

DS recently helped CA obtain access to driver's license data from the National Law Enforcement Telecommunications System, Inc. Access to such data helps us verify driver's licenses submitted in support of passport applications. CA fraud prevention managers now can access state driver's license data from 48 states, Puerto Rico, and the District of Columbia. We continue to work to obtain access to the remaining two states and territories. We will expand the use of this tool by all passport adjudicators in the near future, which also satisfies previous GAO recommendations. Some states have been hesitant to share their data because CA

lacks status as a law enforcement entity for data sharing purposes. We are discussing possible legislation with the Subcommittee on Terrorism, Technology, and Homeland Security of the Senate Judiciary Committee that will grant CA access to law enforcement data for verification purposes.

In addition to the programs above, CA representatives meet regularly with representatives of the intelligence and law enforcement communities to develop strategies to utilize the newest technology and enhance the timely and effective sharing of information. CA also works with DHS Immigration and Customs Enforcement (ICE) Visa Security Unit (VSU) officers who are assigned overseas pursuant to Section 428 of the Homeland Security Act of 2002. VSUs are required by law to review 100 percent of visa applications in Saudi Arabia. ICE/VSUs have also been established at Foreign Service posts in several other countries. CA is working cooperatively with ICE as it considers adding VSUs at additional posts.

Consular Training

Mr. Chairman and distinguished Members, you know that those who wish to do us harm are constantly searching for our weaknesses and vulnerabilities. Therefore, we must ensure that our greatest front-line resource – our consular officers and passport specialists –develops the best skills possible in identifying and uncovering

new fraudulent schemes to obtain U.S. travel documents. Section 7201 (d)(3)(B)(ii) of the Intelligence Reform Act mandates that the Department of State report our efforts to enhance, via training, consular officers' ability to effectively detect and disrupt terrorist travel to the United States. As noted in Congressional findings under Section 7201(a), travel documents are as important to terrorists as weapons. The Department of State is committed to providing the highest level of training to our consular officers, who occupy the key point of control over the issuance of documents valid for travel to the United States.

Presently, there are more than 1,500 consular officer positions in the Foreign Service. Those positions are filled from a larger, mobile, Foreign Service officer workforce, any member of which may at any given time fill a consular or a non-consular position. All officers in consular positions may inspect or review travel or identity documents as part of their official duties. Every single one of those officers is required to have completed the Basic Consular Course prior to performing duties as a consular officer. In addition, whenever an officer returns to consular work after a gap of five years or more, that officer is required to repeat the entire 31-day course.

In fiscal years 2003-2008, more than 500 officers graduated from the Basic Consular Course annually. FY 2009 saw that number grow to 698 as demand and course offerings increased to meet the hiring surge of new Foreign Service and Civil Service personnel. In addition to consular personnel, 59 DS Special Agents completed the Basic Consular Course in FY 2009 in preparation to conduct visa and passport fraud field investigations. Twenty-two agents work in consular sections at overseas posts while the others fill domestic investigative jobs. The Department believes that the Basic Consular Course does an excellent job in addressing the topics mandated under Section 7201(d)(2). The course was lengthened and improved substantially during the past six years, and we are continually reviewing it for further enhancements.

The majority of consular training is offered by FSI. The Basic Consular Course includes modules on the following core consular subjects: Passport and Nationality, Immigrant Visas, Nonimmigrant Visas, American Citizen Services, SAFE (Security, Accountability, Fraud, and Ethics), Interviewing, and Consular Management. The methodology of the course mixes lectures, case studies, practice interviews, hands-on practice with computer applications (including biometric tools), group exercises, graded written examinations, and interagency contact

(including briefings from the CIA and observation of DHS passenger inspection operations at Dulles International Airport).

As noted earlier, the Department of State is scanning fingerprints that are checked against the DHS IDENT watch list and US-VISIT databases, and the FBI's finger-print based criminal history record information administered by the Criminal Justice Information Services Division. At GAO's recommendation, the Department also uses advanced facial recognition technology to screen all immigrant and nonimmigrant visa applicants. To prepare consular officers to use these tools properly and effectively, the Basic Consular Course incorporates extensive hands-on computer training sessions (including the use of the most up-to-date, 10-print biometrics collection technology), integrated throughout the course. In addition to the curriculum material described above, all students in the Basic Consular Course receive personal copies of the 9/11 Commission Report, the 9/11 Commission's Staff Report on Terrorist Travel and the National Strategy to Combat Terrorist Travel.

Additional training courses keep consular officers' skills current and enhance their ability to detect, intercept, and disrupt terrorist travel. The fraud prevention manager course is a one-week course aimed primarily at mid-level consular

officers who are or will be serving as fraud prevention managers in consular sections abroad. One hundred thirty-four officers, including two officers from USCIS's Fraud Detection Laboratory, received the training during FY 2009. We welcome more interagency participation in consular courses.

At the same time that this course was expanded, the content was revised to include new material on the current terrorist threat, briefings by DHS and CA fraud prevention personnel, and other valuable new content, in addition to core skills such as detecting counterfeit documents and consular interviewing. The hands-on anti-fraud technologies curriculum, originally created in 2006, is continually being revised and updated to teach fraud prevention managers how to use Lexis-Nexis, Dun and Bradstreet, and other on-line resources as well as the new anti-fraud tools connected to the CCD.

To date, 1,382 officers and passport adjudicators have successfully completed the mid-level Advanced Consular Namechecking course. The course incorporates new material on biometric technology and use of databases to screen applicants and verify identity. In 2008, we developed a version of the course for use by adjudicators at our domestic passport agencies.

A course for mid-level consular officers on consular interviewing was expanded in October 2007 to include content analysis techniques that can be used during interviews and to assess written statements for use in the overseas and domestic adjudication context. To date, 986 consular officers and passport agency adjudicators have completed the consular interviewing course.

For those officers unable to come to Washington for training, FSI is using distance learning tools to present material on consular fraud prevention and countering terrorist travel. These distance learning tools supplement the Basic Consular Course and subsequent mid-level consular training courses, allowing consular officers to review and refresh their earlier training.

In October 2005, FSI released guidance and a set of specific training modules designed to facilitate orientation and on-the-job training for consular officers newly arrived at their posts of assignment. These modules are designed to identify key topics, but rely on briefers at posts to impart post-specific procedural and other information, much of which is relevant to countering terrorist travel. In August 2009, FSI established a SharePoint website with examples of post-specific training programs and standard operating procedures. This resource is available to all

overseas consular posts and domestic CA officers, and is designed to encourage the sharing and spread of good training practices and procedures.

CA has expanded the National Training Program (NTP), a two-week comprehensive adjudication course that is required for all newly-hired passport specialists. In addition to basic adjudication skills, the NTP includes fraud training and covers topics such as detecting counterfeit documents, identity evidence, analysis of fraud indicators, and fraud resources and referrals. We have also revised the standardized fraud training for passport acceptance agents which now emphasizes identifying an applicant and verifying their identity. We developed a Reference Guide to Counterfeit Documents which provides a quick reference for reviewing a document, understanding its creation, and recognizing the differences between genuine and counterfeit documents.

CA is developing monthly standardized fraud training for passport specialists at each domestic agency and center. The training will include modules on Facial Recognition and Detecting Look-alike Impostors, Foreign Handwriting Detection, Significant Fraud Indicators on Passport Applications, and Delayed Birth Certificate Fraud.

In summary, the Department of State is committed to safeguarding the United States via proper adjudication of visas and U.S. passports. We believe that we have made significant improvements since the attacks of September 11, 2001, but we are constantly looking for ways to do better. As we strive to push our borders outward and seek to interdict terrorists before they ever reach our ports of entry, we have not overlooked the importance of facilitating the travel of legitimate visitors. Advances in technology, data sharing, interagency cooperation, and training, all contribute to a more robust process for screening visa applicants. We have leveraged these same advances to increase the efficiency of the process in order to meet the needs for legitimate travel. We do not view border security and facilitation of travel as goals in opposition. We believe the record of the past seven years shows that we can make advances in both spheres, and we are dedicated to implementing the best possible solutions to further these goals.

Thank you again for the opportunity to be here. I appreciate the Committee's continued interest in our work and have enjoyed the chance to share some of the many accomplishments we have had over the past several years. I am pleased to take your questions.