Testimony
United States Senate Committee on the Judiciary
Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents
May 2, 2007

Andrew Simkin
,

U.S. Senate Committee on the Judiciary Subcommittee on Terrorism, Technology and Homeland Security
Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents

Testimony of Andrew Simkin Director, Office of Fraud Prevention Programs Bureau of Consular Affairs
U.S. Department of State
May 2, 2007
10:00 a.m.

Chairman Feinstein, Ranking Member Kyl, distinguished members of the
Subcommittee:

I appreciate this opportunity to discuss the efforts of the Department of State's Bureau of Consular Affairs (CA) to interrupt terrorist travel. The Department has responsibility for the proper adjudication of passport and visa applications in accordance with U.S. law. Consular officers interview foreign nationals and individuals with claims to U.S. citizenship at over 200 Foreign Service posts around the globe. This is the front line - the first and probably the best opportunity to detect deception and prevent a terrorist or other criminal from traveling to our country.

Secure Travel Documents

The 9111 Commission noted that travel documents are as valuable as weapons to terrorists. Altered passports and visas, or genuine documents obtained fraudulently, allow terrorists - and other criminals - to cross borders in the course of planning or carrying out operations.

U.S. passports and visas are among the most valuable and highly sought-after travel documents in the world. Demand for them is high, and rising. The Department issued 12.1 million U.S. passports in FY 2006, an all-time record. We anticipate issuing more than 17 million this year. We issued 5.8 million nonimmigrant visas in FY 2006 - 8.3 percent more than in 2005 - while refusing visas to 1.9 million visa applicants.

The Department is committed to ensuring that U.S. citizens have passports when they need to travel and to providing transparent, efficient visa adjudication for legitimate tourists, business visitors, students, and other travelers, whose visits to the United States we encourage and value. At the same time, we will not compromise our commitment to the security of such documents and the integrity of the consular adjudication processes.

Passports

On August 14, 2006, at our Colorado Passport Agency, the Department of State began issuing to the public a redesigned U.S. passport that for the first time includes facial recognition biometrics and a contactless chip embedded in the book. These "e-passports" are the most secure U.S. passport ever produced and represent a major enhancement in ensuring the integrity of travel documents.

We adopted a multi-layered approach in designing the e-passport in order to implement higher security standards, address privacy concerns, and protect personal data. The result is a document that is considerably more difficult to counterfeit or for an impostor to use should it be lost or stolen.

A digitized photo of the bearer on the data page is the standard passport biometric adopted by the International Civil Aviation Association (lCAO). A radio frequency identification (RFID) microchip embedded in the back cover contains the same identifying information printed on the data page of the passport - name, date of birth, gender, place of birth, dates of passport issuance and expiration, passport number, and the digitized photo image of the bearer. The data written to the chip is protected from alteration by the use of a Public Key Infrastructure (PKI) digital signature.

The e-passport incorporates other overlapping security measures to protect the bearer's privacy and secure personal data. Metallic webbing in the front cover and spine of the book prevents surreptitious "skimming" of the data on the chip while the book is closed. This is complemented by Basic Access Control (BAC) technology, which requires that the passport's machine-readable zone be read in order to generate the electronic key that unlocks the chip. To address the concern that the RFID chip might be used to track the bearer, we employed Randomized Unique Chip Identifiers (RUIDs), which generate a different ID number each time the chip is read by a passport chip reader.

With traditional passports, two things must match in a legitimate case: the face of the bearer and the data on the photo page. Detection of photo substitution or other tampering is dependent upon the border inspector's training and expertise. With the e-passport, three things must match to confirm that the traveler is the person to whom the passport was issued: the face of the traveler, the data on the photo page, and the data on the chip. The immigration inspector scans the passport and, in a matter of seconds, will be able to confirm the identity of the passport bearer. Border authorities can better intercept suspect travelers and speed entry of legitimate travelers. Further, border authorities in other countries can in effect assist us in managing the integrity of e-passports each time they report instances when the three elements don't match.

In developing the e-passport, we consulted frequently with industry experts and solicited public comments through the Federal Register before beginning production. We conducted rigorous tests of the chip's security with technical experts from the private sector and the National Institute of Standards and Technology to assess the risk of unauthorized reading and to evaluate the efficacy of countermeasures. We are confident that unauthorized individuals will not be able to extract information from the chips.

To date, we have issued three million U.S. e-passports. All of our domestic passport agencies and one passport center have been fully converted to issue e-passports. Conversion of the one remaining passport center should be completed later this month.

When reviewing our passport operations, we identified emergency passports - those issued by posts overseas to replace lost or stolen passports for U.S. citizens - as a potential vulnerability in the passport security program because such passports used glued or laminated photos of the bearer, which are easier to substitute or alter than digitized photos. We have replaced the old passports with a more secure photo-digitized passport. We launched the Emergency Photo-Digitized Passport (EPDP) in fall 2006. Since February 2007, U.S. embassies and consulates issue only the EPDP in emergency cases.

The data for an EPDP are printed on a secure foil - similar to that used for U.S. visas - which is then sealed to a page by a heat laminate that is difficult to alter without destroying the laminate or data page. Digital security fields incorporated into the foil encode data viewable only with a special lens or decoding software. An additional data coding scheme indicates tampering if the data page is modified.

I would be happy to share with the Subcommittee samples of the e-passport and the EPDP.

In anticipation of the implementation of the land border phase of the Western Hemisphere Travel Initiative (WHTI), and to meet the unique needs of the border community, the Department is also developing, in coordination with the Department of Homeland Security (DHS), a limited-use passport card as a secure alternative document to the traditional passport book.

The convenient wallet-sized card will contain a vicinity-read RFID electronic chip to meet the operational needs at DHS ports of entry (POEs). State-of-the- art security features will be used to reduce the risk of counterfeiting or forgery. The chip will contain a unique identifier number rather than sensitive personal data. The number will be linked to a secure database maintained by the Departments of Homeland Security and State.

We are aware that vicinity-read RFID technology has raised concerns about data privacy, and we are working actively with industry to address those concerns. We are committed to providing a durable and highly secure passport card to the American public.

Visas

The Department has incorporated biometric technology - specifically, facial recognition and fingerprint scans - into U.S. visa processes as well. The U.S. BioVisa program is completely integrated with the DHS US-VISIT program, so that anyone entering the United States on a nonimmigrant visa can be identified through biometrics.

All visa applicants submit a photo with the application. A digitized image of the photo is included on the visa, as well as in the electronic visa record. In September 2003, we began deploying fingerprint scanners to overseas posts, and by October 2004, all posts were collecting electronic fingerprints, thus meeting the statutory deadline established by the Enhanced Border Security and Visa Entry Reform Act of 2002. We collect two fingerprints from each visa applicant (other than for diplomats and those under the age of 14 or over 79). Prior to visa issuance, the fingerprints are cleared against the DHS Automated Biometric Identification System (IDENT), which contains fingerprints of known or suspected terrorists (KSTs) and of persons wanted by law enforcement. We have cleared fingerprints of over 17 million visa applicants through IDENT. Over 35,000 IDENT matches have been investigated by consular officers and, where appropriate, have resulted in visa denials. More recently, we have successfully completed a pilot test of a new process for electronically collecting 10 fingerprints, rather than two. Ten fingerprints provide a greater number of data points, allowing more complete checks against criminal history fingerprint records and much more accurate responses. We have begun rolling out this technology to posts, and we expect to complete worldwide deployment by the end of 2007.

Passport and Visa Adjudication Processes

Even more important than the security of documents themselves is the integrity of the adjudication process, including the electronic databases used to screen applicants and verify their status. All valid U.S. passports are supported by PIERS, a database of passport records, including photos, applications, and history, which 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.

The Consular Lost and Stolen Passports (CLASP)' database includes over 1.3 million records concerning U.S. passports. All passport applications are checked against CLASP, PIERS, the Social Security Administration's database, and the Consular Lookout and Support System (CLASS), which includes information provided by the Department of Health and Human Services (HHS) and law enforcement agencies such as the Federal Bureau of Investigations (FBI) and U.S. Marshals Service.

Every visa applicant also undergoes extensive security checks before a visa can be issued. Our system automatically runs a name-based check in a database that currently includes more than 20 million entries. These entries include State Department information, FBI files, immigration violations, and intelligence from other agencies. All visa applications are checked against derogatory information of KSTs in the Terrorist Screening Database (TSDB). The TSDB integrates terrorist watchlists from all U.S. Government (USG) sources. It is maintained by the Terrorist Screening Center (TSC), which serves as the centralized point of contact for hits against the watchlists. Hits are reviewed by USG agencies in Washington, D.C., prior to any visa being approved. New KST entries are checked against records of previously issued valid visas, enabling us to prudentially revoke those visas. Since 9/11, we have revoked more than 1,700 visas of individuals suspected of being connected to terrorism.

Our consular lookout database contains information from past findings of visa ineligibility as well as information from other agencies. When a consular officer determines that an applicant matches a "hit" in the database, or if the applicant meets other established criteria, the case is referred for an interagency security review in Washington, D.C., resulting in a Security Advisory Opinion (SAO) sent back to the consular officer. We processed nearly 245,000 SAOs in FY 2006, and over one million since 9/11.

The Consular Visa Interview

One of the most significant changes in consular practice after September 11 was a re-emphasis on the personal interview. The interview is the best available tool for detecting an applicant who has criminal intentions but whose name, fingerprints, and photo do not match any derogatory information previously known to the U.S. Government.

In these interactions, the consular officer has an inherent advantage in that the mala fide applicant, in preparing a cover story for his mala fide travel, cannot possibly plan and memorize answers to all of the infinite variety of questions that the consular officer may ask. Furthermore, per section 291 of the Immigration and Nationality Act, the burden of proof is on the visa applicant. Per section 214(b) of that Act, if the applicant does not establish his eligibility for a visa to the satisfaction of the consular officer, then the visa must be denied.

Making these decisions demands every bit of preparation that the consular officer can bring to bear in terms of intellect, foreign language skill, human understanding, cultural awareness, and judgment. We cannot guarantee that every terrorist will be detected and denied by an alert consular officer. However, the array of measures we have put in place, including analytic interviewing techniques, biometric checks, database checks, and document verification, poses a significant obstacle and deterrent to persons seeking entry to the United States to do us harm.

Other Fraud Prevention Techniques

We have a variety of tools available, in addition to the consular interview, to separate fact from fiction in visa applications. Consular Fraud Prevention Managers and locally-engaged staff conduct field inquiries, visit Civil Registries, telephone employers or schools, and consult local contacts. We employ increasingly sophisticated electronic search capabilities to detect links between different fraudulent cases or to check an applicant's story against available sources of data. Consular officers often consult Internet resources including maps and satellite photos to verify the information contained in visa applications.

Our principal goal in these endeavors is to reach the right decision regarding the visa or passport application. Often, however, we run across organized or egregious 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 and may be assigned as overseas criminal investigators based in the consular section at a Foreign Service post. In many cases, based on DS's excellent liaison relationships with local police, a perpetrator of fraud not only is rejected for a visa, but is then placed under arrest at the front gate on departing the Embassy. I believe that this coordination with DS is a very powerful factor in deterring terrorist attempts to secure visas, as well as deterring other kinds of fraud.

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

CA also works with Immigration and Customs Enforcement Visa Security Unit (ICENSU) officers who are assigned overseas as mandated by section 428 of the Homeland Security Act of2002. Visa Security Units are required to review 100 percent of visa applications in Saudi Arabia. CA is working cooperatively with ICENSU as they consider expanding to additional posts.

Enhanced Training for Consular Officers

Given the key point of control that consular officers occupy in screening U.S. travel documents, the Bureau of Consular Affairs accords the highest priority to providing comprehensive training to consular officers. Working with the Department of State's Foreign Service Institute, we have expanded and updated basic and continuing training programs for consular officers, with a particular focus on anti-fraud measures.

There are currently more than 1,600 consular officer positions. The Department of State created 570 of these since 9/11 to increase the resources dedicated to consular adjudication.

Every officer assigned to serve a consular tour must first complete the 31- day Basic Consular Course, and any officer returning to consular work after performing non-consular work for five years or more is required to repeat the course. In addition to covering the core consular subjects of passports, visas, American citizen services, consular interviewing, and consular management, the course has been enhanced to include lessons learned from 9/11. It includes briefings and hands-on analysis of documents to help students practice recognizing the security features of genuine travel documents and indicators of altered and counterfeit documents. Trainees also learn to detect impostors who may present genuine documents not legitimately belonging to them. Since 2003, the course has included training in interview techniques designed to spot inconsistencies in an applicant's story or demeanor and the micro facial inflections applicants may betray when experiencing emotions during the interview.

Additional training courses beyond the Basic Consular Course keep consular officers current and enhance their ability to detect, intercept, and disrupt terrorist travel. In conjunction with FSI, we have accomplished the following:

- Created a new course, Advanced Consular Namechecking, to provide visa officers a detailed understanding of the results from the various lookout systems (including namechecks, biometrics, and facial recognition). Since 2002, when the course was first introduced, 709 consular officers have attended this four-day course, and an additional 107 officers have attended a one-day version offered overseas.

• Established a new one-day course on Consular Interviewing to ensure that mid-level consular managers have access to new content on detecting deception which was added to the Basic Consular Course. To date, 625 consular officers and passport examiners have taken this course.

• Expanded offerings of the five-day Fraud Prevention for Consular Managers course from two to eight per year, increasing enrollments from 42 in FY 2004 to 185 in FY 2006. The course curriculum includes a briefing on terrorist travel, hands-on training in use of classified SIPRnet resources and unclassified USG and commercial databases, briefings from DHS, and instruction on document analysis.

• Launched distance learning courses on Detecting Impostors, Detecting Fraudulent Documents, and Examining U.S. Passports. Consular personnel all over the world, as well as other personnel such as diplomatic security special agents and other agency officials can now access these courses from their desktops.

• Sponsored regional fraud prevention conferences for consular officers assigned to the Middle East, the Western Hemisphere, East Asia, Europe, and Africa. Fraud prevention training has also been incorporated into nine regional Consular Leadership Development Conferences (CLDCs) during FY 2006 and FY 2007.

In addition to formal fraud training provided to officers and locally employed staff, CA's Office of Fraud Prevention Programs assists posts in continuously improving fraud prevention and detection techniques by analyzing and sharing fraud information, providing consular officers with access to advanced databases and other technological tools, and liaising with other agencies.

Information Sharing

Developing secure travel documents and training our staff are important tools in disrupting terrorist travel. As the 9/11 Commission noted, this effort also requires collaboration with other nations. The Department recognizes that routine and timely information sharing within the USG, with international organizations, and with other governments is critical to success, and we are pursuing this aggressively on a number of fronts.

Interagency Datashare

CLASS continues to operate its well-tuned, two-way sharing of lookout names with the DHS Treasury Enforcement Communications System (TECS), which is used at ports of entry. The overall CLASS database of names has risen to over 20 million records in recent years, including millions of names of criminals from FBI records provided to the State Department under the terms of the USA PATRIOT Act.

Up to 35,000 files on issued visas are transferred daily to TECS within minutes of issuance at posts around the world, while fingerprints collected with these visas are transferred to the DHS IDENT fingerprint system. In addition to sending data to TECS and IDENT, CA has actively shared with other agencies access to its consular consolidated database (CCD). Over 8,000 users from DS, DHS, FBI, the Departments of Commerce, Defense, and Justice, and other U.S. Government agencies have access to the CCD, making over one million queries per month.

Datashare with International Organizations

In 2004, the Department began transferring data on U.S. lost and stolen passports to Interpol. We have shared all the data we have - more than 1.3 million records. The United States is the largest single contributor of lost and stolen passport data to Interpol's Automated Search Facility/Stolen and Lost Travel

Document Database (ASF/SLTD). This database contains more than 14 million recorded lost/stolen documents.

Access to records in the Interpol system is not automatic or in real time. An immigration or border official must suspect the authenticity of a traveler's documentation and in each case query the Interpol database. The Department recognizes the need to establish a systematic and routine mechanism for widespread use of the Interpol database at U.S. Foreign Service posts and POEs. The primary challenge is developing access architecture that would support the volume of queries involved and the ability to get responses in real or near-real time.

Information Sharing with Other Governments

Another vital aspect of disrupting terrorist travel involves international sharing of information on terrorists. Within the Department of State, the Bureau of Consular Affairs has the lead on negotiating with foreign governments for the international sharing of terrorist lookout information, under authority delegated pursuant to Homeland Security Presidential Directive Number 6 (HSPD-6). The United States has pre-existing agreements that satisfy the requirements ofHSPD-6 with Australia and Canada. We have approached all 27 countries currently participating in the Visa Waiver Program, as well as a limited number of other key partners.

We have signed HSPD-6 agreements with three countries and are finalizing the technical details for beginning the data exchanges. We are engaged in working level discussions with 10 countries and have received serious expressions of interest from six others. The goal of these arrangements is to ensure the timely receipt of information on KSTs before they travel, so that consular officers, POE inspectors, and others can make informed, accurate, timely decisions and disrupt the travel of potential terrorists.

Conclusion

Madam Chairwoman, we are focused on maintaining the security of U.S. travel documents, while optimizing the technology, procedures, information, and training that go into the issuance and verification of travel documents. Consular officers occupy the front line in interrupting terrorist travel. At the same time, we may be the first American officials that millions of legitimate travelers meet. The impression that we make may well form a lasting opinion of America in their minds. We are thus responsible for securing our country and for serving as its public face. It is an honor to carry these responsibilities, and we will continue to do so to the very best of our abilities.