

Testimony of  
**Ms. Janice Jacobs**

July 15, 2003

United States Senate Committee on the Judiciary  
Subcommittee on Immigration  
Hearing on Information Sharing  
Testimony of Janice L. Jacobs  
Deputy Assistant Secretary of State  
For Visa Services  
July 15, 2003

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to address you on a subject that all of us in the executive and legislative branch agree is crucial: the swift and proper exchange of information among relevant agencies controlling the security of our borders. The Department of State's visa work abroad constitutes the "forward based defense" of the United States against terrorists and criminals who seek to enter the country to harm us. We have no higher responsibility and we are determined to do this work in the best and most comprehensive manner possible. The General Accounting Office has issued a number of reports touching upon this subject, and the three we have just heard GAO speak to are very familiar to us at State. We have found them to be thoughtful studies of a complex subject and we have learned from them and put many of their recommendations into effect.

The GAO report from October of 2002 entitled "Visa Process Should Be Strengthened As An Anti-Terrorism Tool" made a number of excellent recommendations that we have used as a sort of roadmap for implementing the changes that more perilous times demand of us. I have appended to my written statement a substantial list of actions taken since September 11 to strengthen the visa process along the lines suggested by GAO. Let me summarize them quickly here: we have doubled our database holdings on individuals who should not be issued visas, increased our training efforts to better apprise consular officers of counter-terrorism issues, increased data-sharing capabilities among federal agencies, set up special programs to more fully vet visa applicants of particular concern, and moved to increase staffing for visa positions abroad. Our training efforts have focused on needed counter-terrorism expertise and we have devoted much more time in senior training for Ambassadors and Deputy Chiefs of Mission to consular work and its responsibilities for senior managers. We have thoroughly reviewed consular procedures on visa work and begun a series of Standard Operating Procedures cables to the field to codify the way in which we expect visa work to be consistently performed abroad. While you never achieve perfection in this area, I am confident that we have a much stronger visa process in place at our posts overseas than we had just one year ago and the country is safer for it.

There is a cost to all of this effort and it is not simply born by the Department in terms of greater personnel and equipment needs. It also comes at a cost in time and a certain amount of inconvenience to visa applicants who now must navigate a process that is more burdensome than it has been in the past. Secretary Powell has succinctly articulated our policy as "Secure Borders, Open Doors", and we at the Department are acutely aware of the need to satisfy both of these objectives. The US economy counts on the billions of dollars spent each year by international tourists, our universities reap the economic benefits of pre-eminence among destination countries for international students, our scientific establishment flourishes in a climate of open exchange across borders, and our entire society is accustomed to living in a free and open manner that counts upon an ease of movement across international borders. We are determined to preserve these crucial benefits to the United States even as we work to strengthen the visa process' security.

Secretary Powell has also said to the Congress that we are only as good on visa lines as the information we have available to us on threats to the United States. I of course agree completely with this observation, and the Department greeted the report done by GAO in April of this year ("Terrorist Watch Lists Should Be Consolidated to Promote Better Integration and Sharing" GAO-03-322) on this theme with its full endorsement. While none of the 9/11 hijackers would have been identified by a unified watch list, since they were not known to us prior to their visa applications, swift provision of all the best information known to the US government from whatever source to our line visa officers is essential to ensure that we stop those dangerous persons who are identified by our various agencies.

This particular GAO report charges the new Department of Homeland Security with working with other agency heads and departments to design a consolidated and standardized "watch list" that can be unified and shared among the agencies that need this information, and it also suggests that DHS is best placed to know who might need such access among the universe of potential end users. Again we agree that DHS is the place where such an effort ought to be vested, and we pledge our full support for such an essential project. The GAO speaks of "cultural differences" as being among the chief reasons for variation in the sharing of such lists among the federal agencies. While I would not deny that "cultures" unique to a particular federal agency condition its work, I think that what the GAO really means is that the mission of each federal agency is distinct and the need for and ability to use certain information is different among them.

A consular officer abroad, who has as much time as he needs to review a visa applicant and can send that applicant home to bring in more information if needed, is in a much different situation than a Port of Entry inspector who has a few minutes to decide whether or not to admit an alien to the United States. Our consular officer can use information that is less conclusive than the inspector would require, and a law enforcement officer in the United States will have somewhat different requirements than either of those two officials. While it is obviously right to err on the side of caution when dealing with potentially lethal security risks, we cannot eliminate every element of risk from our operations, and saddling certain officials with information that experience tells us they cannot use effectively, either because of legal or operational requirements, will not enhance our border security. These are questions without easy answers, but we believe that DHS is best placed to consider them, and broker intelligent solutions based on the contributions of the interested agencies.

Finally, let me address the question of visa revocations that was studied by the GAO in yet a third report (New Policies and Procedures Are Needed to Fill Gaps in the Visa Revocation Process; GAO 03-798). The GAO correctly identified a problem in our failure to rapidly and certainly apprise our border inspection and law enforcement agencies of "prudential revocations" that we had made based on intelligence and other source identifications of potential security threats. Our procedures were insufficiently systematic and our notifications did not make use of the best our technology can deliver. The problem though has been fixed in the creation last year of a revocation code that is shared out to the relevant agencies via the Inter-Agency Border Inspection System (IBIS) when a visa is prudentially revoked. Though it should have been fully operational in August of 2002 when we designed the code, it was put into place in December of that year, and we have verified that each and every revocation for calendar year 2003 was properly coded and entered into CLASS and IBIS and was available in near real time to our law enforcement and border inspection colleagues.

The question of when a prudential revocation takes effect, while somewhat complex legally, is pretty straight-forward operationally. A prudential revocation of a visa is just that: a safety precaution that, in security cases, we undertake with a relatively low threshold of information to ensure that all relevant or potentially relevant facts about an alien are thoroughly explored before we admit that alien to the United States. It is a signal to the consular officer abroad to re-adjudicate the case with the new information at hand. In many such instances we find that the information does not pertain to the alien whose visa was revoked (a mistaken identity due to incomplete identifying data), or that the information can be explained in a way that clarifies the question at hand and eliminates the potential threat. In these cases we re-issue the visa and purge the alien's name from the lookout system.

The Department of State has advised the Department of Homeland Security that it is prepared to begin revoking visas effective immediately in cases of aliens who present a valid visa to an immigration inspector at a port-of-entry but of whom DHS nevertheless has security concerns resulting from a more in-depth inspection. We will institute this practice on a routine basis once we have developed implementation procedures with DHS; meanwhile, we can consider cases on an individual basis. Making a revocation effective immediately when the alien is at the port-of-entry will allow DHS to use expedited exclusion procedures appropriate to the nature of the potential threat. Because the alien's visa will have been invalidated, DHS will be able to deny the alien admission to the United States under INA 212(a)(7)(lack of a valid visa). Thus, as in the cases of aliens outside the United States, the visa revocation will eliminate the need for DHS to establish that the alien is ineligible for admission under one of the security grounds of exclusion in Section 240 removal proceedings, which could require the disclosure of classified information.

A third situation arises if the alien has already been admitted to the United States. In this context, there is no legal precedent indicating that, if a visa were revoked effective immediately, it would facilitate DHS's ability to remove the alien from the United States. For example, it is unclear what removal charges could be filed against the alien. We intend to discuss this matter further with DHS as well as with the Department of Justice.

I can assure this subcommittee that in all of these areas we work hand in glove with our colleagues in law enforcement and homeland security. There are no cultural differences in each

of our determination to make the United States safe from terrorists and criminals for Americans and our foreign guests. We have made great strides in information sharing and cooperation towards this end, but we clearly have a way to go. I would be glad to answer any questions you may have. Thank you.

Attachment: Bureau of Consular Affairs  
Accomplishments in FY 2002/2003

Bureau of Consular Affairs  
Accomplishments in FY 2002/2003

In FY 2002-2003, the Bureau of Consular Affairs (CA):

- ? Set a worldwide standard for visa interview policy.
- ? Tightened visa interview requirements for nationals of state sponsors of terrorism.
- ? Instituted specialized training for consular officers in determining deception through a visa

interview at the National Foreign Affairs Training Center.

? Incorporated over 7 million records from the FBI's National Crime Information Center (NCIC) into the Consular Lookout and Support System (CLASS) namecheck database, nearly doubling the size of CLASS to 13 million records.

? Received into CLASS a threefold increase in namecheck records from the intelligence community (through the Bureau of Intelligence and Research's TIPOFF office).

? Provided access to the Consular Consolidated Database (CCD) to consular officers worldwide, as well as to the Department of Homeland Security's ports of entry and a military intelligence entity.

? Mandated that each post review consular management practices and utilized the results in developing and transmitting a series of cables providing standard operating procedures (SOP) to the field to standardize consular practices worldwide.

? Broadened cooperation with the Bureau of Diplomatic Security (DS), creating a vulnerability assessment unit in CA to alert us to possible malfeasance trends through statistical analysis.

? Organized Consular Management Assistance Teams (CMATs) to visit, assess, and provide guidance to posts in strengthening consular management practices.

? Continued to expand entries to our Foreign Lost and Stolen Passport Database and expanded electronic sharing of this information with U.S. ports of entry.

? Deployed the new, tamper-resistant Lincoln visa worldwide to prevent alteration and duplication.

? Increased datasharing with the intel and law enforcement community.

? Automated crosschecking of new derogatory information (i.e. lookout list entries) against records of previously issued visas.

? Broadened the definition of terrorism for visa denial purposes.

? Added more interagency security checks for counter-terrorism purposes known as "Visas Condor".

? Implemented a new supplemental visa application form of all men ages 16 to 45 from every country in the world.

? Engaged in ongoing discussions with Mexico and Canada about greater cooperation on immigration, security, and visa issues.

? Closed a loophole that allowed certain non-immigrant aliens to re-enter the U.S. with an expired visa.

? Issued a proposed rule in the Federal Register for the elimination of the crew list visa.

? Improved the system for exchanging background check data with the FBI.

? Implemented a training program for consular officers to better understand the CLASS system, especially linguistically-based namecheck returns, and expanded intranet resources to assist officers in reading entry/exit cachets in Arabic or Persian script.

? Deployed the latest Nonimmigrant Visa (NIV) software release incorporating enhanced data collection and improved scanning features to help with security-related tasks.

? Developed a more secure way of canceling machine-readable visas to deter "visa washing."

? Released an update of the NIV software, which incorporates imaging of serious visa refusals into the CCD.

? Provided the National Institute of Standards and Technology with over a million photographs of visa applicants for use in their facial recognition evaluation tests and continued work on biometric identifier standards and electronic systems.

? Approved an Entry-Exit Project Charter, drafted jointly with INS, Customs, and DOT, that sets

the parameters for an automated system to record the arrivals, departures, and stay activities of individuals coming to and leaving the U.S.

? Commenced programs to increase document fraud training for Diplomatic Security agents, and with SSA to improve document fraud training for SSA special investigators.

? Compiled a "Law Enforcement Package" that Diplomatic Security field offices, Passport Agencies, or other DOS offices may provide to state and local law enforcement contacts or to banks or other businesses requesting general guidance on assessing U.S. visas and passports as identity documents.

? Launched the Interim Student and Exchange Authentication System, which provided for the electronic verification of foreign students and exchange visitors applying to enter the U.S.

329,831 records were entered into ISEAS from 6,720 organizations before it sunset on March 31, 2003, with the advent of the DHS Student and Exchange Visitor Information System (SEVIS).

? Began participation in the European Union fraudulent documents working group, sharing information on smuggling trends, fraud patterns and document fixers.

? Launched a facial recognition pilot in April 2003 for nonimmigrant visas.

? Developed global standards for passport issuance security, which were adopted by the G 8 countries.

? Began working with DHS to institute a prevent-departure system to assist in preventing an alien parent or alien child from leaving the country when international child abduction is suspected.