



220 I Street, NW, Suite 220

Washington, DC 20002

(202)544-0004

Fax: (202) 544-0004

www.immigrationforum.org

Making Our Immigration System More Secure to Guard Against Terrorism

As Congress and the Administration consider ways to prevent a recurrence of the tragic events of September 11th, strengthening aspects of our immigration system will be a part of the mix of recommendations that will come out of ongoing deliberations. There are many ways that we can better screen the individuals seeking entry to the U.S. However, *any change in the way we manage our immigration system will have only a limited impact on our national security.* Far more important is our capacity to collect and analyze intelligence. Unless we know who it is that seeks to do us harm and make sure that information is in the hands of the proper authorities, the immigration system will be unable to catch these individuals.

Congress must be careful not to overreact and pass proposals that will in effect isolate the U.S., but do nothing to increase our security. Proposals that would make it much more difficult for all foreigners to enter may make us *less* secure, if resources that could be used to detect and screen potential terrorists are diverted by methods that have as their foundation the assumption that *all* foreigners are potential terrorists. Similarly, Congress should resist proposals that would so slow the flow of commerce across borders that they would, in effect, put an embargo on our economy.

Below are suggestions for steps that can be taken to increase the likelihood that potential terrorists would be caught before they act.

Human Intelligence and Technology.

Intelligence is Key. All federal law enforcement agencies collect the names of persons who should not be admitted to the U.S., or who should be pulled aside for additional questioning. These are individuals who have criminal records, who were denied visas in the past, who have been previously deported, who may be wanted on drug charges, who are suspected to have connections to terrorism, or who have otherwise been identified as suspect or questionable in some other way. Millions of names have been collected. For this data to be as useful as it could be, intelligence agencies and law enforcement agencies must share the latest intelligence among themselves, consolidate their lists, and update the information as soon as possible after it is obtained. Currently, some sensitive information collected by intelligence agencies is not shared with all U.S. authorities who should have access to this information. So, for example, some U.S. consulates abroad—the State Department offices that issue visas to individuals traveling to the U.S.—do not have access to complete information on individuals who should be denied entry to the U.S.

In light of our security needs in the aftermath of the September 11th terrorist attacks, there should be an overall review of which databases are relevant to potentially increasing our security, who should appropriately have access to these databases, and how to guard against abuses that might arise with greater access to these databases so that our civil liberties and privacy can be balanced with our need for security.

Need for Safeguards. With so many names on the lookout list, there must be a procedure for removing someone from the list, or ensuring that someone with the same or similar name as someone on the list can enter the U.S. after it has been ascertained that they are not the actual person with whom authorities are concerned. This problem will become more acute as more names are added to the list, and as it becomes easier for various law enforcement entities to add names to the list. Part of the problem is that unfamiliar names from various regions of the world are often keyed in to a database incorrectly. We must make every effort to ensure the accuracy of names on the list, to ensure that we are not going after the wrong individuals. Until biometric identifiers are included in what we collect from those arriving to the U.S., we may need to collect additional information from those entering in order to reduce the incidence of mistaken identity.

New Technologies to Verify Identities. Weaknesses in the lookout system include the ability of potential terrorists to use aliases or obtain false identification and, as noted above, the fact that many people who are not sought by authorities have similar names to those on the list. Ultimately, the lookout list will be made more secure with the addition of promising new technologies that can match a unique identifying characteristic of an individual with a name. One promising new technology is a face recognition system that uses cameras to scan a person's face and compare the picture with a database containing the photos of persons who authorities suspect. This technology has been tested successfully, leading to the apprehension of several persons wanted on various criminal warrants. This technology is relatively non-intrusive, compared to, for example, a fingerprint check. The camera can scan from a distance. Images need not be retained (unlike, say, the camera at an automated teller machine), but only compared to a database of images. That database would not contain the images of law-abiding citizens, but only those of persons the authorities are looking for. Finally, the technology is relatively inexpensive, and could be effectively employed at ports of entry, both at the point of inspection and at points of access to secure areas. Still, before this kind of surveillance technology is used as a matter of routine, important privacy and civil liberties questions will have to be addressed, and uses of the facial image database should be limited to national security or criminal law enforcement.

Like the lookout list, the successful use of this technology will increase as our human intelligence improves, and as photos of persons authorities are looking for are added to the database.

Make Travel Documents More Secure. In addition to the sharing of information, all countries should be encouraged to increase the security of the issuance of passports, to make them more difficult to forge. Machine-readable passports would make it more difficult to counterfeit a passport. With machine-readable passports, the information on the passport is digitized, and appears on the screen of the immigration inspector, and thus serves as a check against attempts to alter the passport. Including the digitized image on the passport would make the document more secure, as the photo of the person the passport was issued to would appear on the screen of the computer reading the passport. The inspector would then compare the digitized image with the person in front of him. An additional layer of security might be built into the system if the U.S. moved to issue machine-readable visas, with a digitized image of the person who the visa was issued to. This would make it easier to ascertain a continuum of identity—the person the passport was issued to, the person who obtained the visa, and the person entering the country are the same person. The State Department is now issuing machine-readable visas, but in most ports of entry, the machines to read these visas are not in place.

Countries whose citizens are not required to obtain visas to enter the U.S. for 90 days or less (in the "visa waiver" program) are required to develop machine-readable passports by 2007 if they wish to remain eligible to continue in the visa waiver program. In light of the urgency created by the terrorist attacks, this deadline should be moved up. Beyond this feature, the standardization of passports among nations would

make fraud detection easier. Specifications for machine-readable passports are being developed by the 187-member-nation International Civil Aviation Organization. Specifications should be agreed upon and implemented.

More immediately, information about stolen passports should be shared among governments, as the theft and sale of passports from visa waiver countries is an increasing problem. These governments should share information on all stolen passports. The practice up to now has been to report only passports that are stolen in large batches.

Nothing Will Work Without Funding. The government already has an arsenal of tools to increase our security. However, the agencies and offices charged with carrying out security responsibilities are often under-funded. For example, both the Department of State and the Immigration and Naturalization Service (INS) must have increased funding to upgrade their technological infrastructure, and beef up their staff charged with collecting and analyzing intelligence data. Both agencies should have the latest computer technology, and both agencies should be able to access information from each other.

Of course, any new technology and human intelligence capacity that results from our current deliberations will take a commitment of funding above and beyond the funding needed to fully implement the present tools available to federal agencies. An increase in technological capacity will require an increase in capacity to analyze and interpret data effectively. This will involve employing experienced agents who will have to be paid at a level reflecting that experience.

Finally, there will have to be a commitment to employ enough staff to use all of that information to determine in a timely manner whether the hundreds of millions of persons seeking entry to the U.S. should be admitted or kept out.

Screening Individuals Before They Arrive in the U.S.

Consular Offices: The First Line of Defense. When a person wishes to come to the U.S. legally, he or she must first apply for a visa from a U.S. consulate abroad (except for nationals of countries in the visa waiver program who are coming for brief periods of time). A consular officer interviews the applicant, and assesses whether the applicant is admissible or whether the applicant would likely violate the terms of a visa once here. Currently, the personnel charged with examining visa applicants and making these decisions tend to be more junior personnel, with little experience. These officers must deal with a high volume of applications, and must make a decision on the basis of a brief interview. There is little prestige in this work, and the focus of the visa adjudication process has been more to screen out individuals who really intend to stay in the U.S. permanently (“intending immigrants”). Inexperience, combined with difficult circumstances and perhaps a flawed emphasis in the screening process, increases the likelihood that a mistake will be made and someone who seeks to do us harm will be granted a visa.

In the effort to increase our security, we will have to consider changing the screening process, the way it is staffed, and the expectations of visa applicants themselves. There will have to be a shift in the process so there is less emphasis on weeding out intending immigrants and more emphasis on weeding out potential terrorists. The adjudication of visas might be accomplished by a dedicated consular corps, specializing in evaluating visa applications, and not using the job merely as a stepping-stone to more prestigious and better-paying positions in the foreign service. Finally, we may have to change the expectations of visa applicants. The adjudication process may require a more thorough background check, and it may no longer be wise to approve a visa on the spot.

Immigration Checks at Airports Abroad. For the most part, people traveling to the U.S. are inspected by immigration officers at the point of arrival in the U.S., at international airports here. In some high-volume airports abroad, U.S. immigration checks are performed at the point of departure. That is, a passport is inspected and the name is run against the lookout list *before* the individual boards a plane to the U.S. A system for screening for inadmissible persons at the point of departure allows more time for inspection—and increases the likelihood of a more thorough check—than is possible when a plane-load of passengers gets off the plane in the U.S. (The INS is required to inspect all passengers of an offloading plane within a 45-minute timeframe.) An expansion of these pre-inspection sites to other high-volume airports might be considered. While a U.S. inspector does not have authority to apprehend someone should he come across a suspected terrorist, the U.S. can work cooperatively with authorities at the pre-clearance site who have the power to arrest and detain. Establishing these pre-inspection sites has been expensive and, up to now, difficult to negotiate with the host country. It may be that the September 11 incident will bring about a greater spirit of cooperation, given the worldwide nature of the terrorist threat. Such cooperation should include assurances that suspected terrorists are not merely released because authorities in the host country do not view the threat as seriously as the U.S. does.

A North American System. The United States must employ multilateral strategies in all aspects of combating terrorism, not the least of which is partnering with Canada and Mexico in creating a North American perimeter that will bolster security through law enforcement coordination, intelligence sharing, and better joint use of enforcement resources. Closer cooperation with our North American neighbors might include a better understanding of our mutual security concerns, so that those issues are taken into account in the issuance of visas and in the asylum process. Such coordination and cooperation would reduce the chance that someone wishing to do harm to the U.S. would travel to one of our neighboring countries and then cross by land to the U.S.

On our border with Mexico, the U.S. has dedicated more personnel to border security in the past several years. As a result, crossing the Southwest border has become more daunting. Criminal smuggling rings, with knowledge of the weaknesses in our border security, have developed into a multi-billion-dollar-a-year business, as people intent on crossing the border illegally turn to smugglers to aid them in their effort to cross. Potential terrorists might use these smuggling operations to cross the border in a way that evades detection. Detecting and striking against smuggling operations will take cross-border cooperation, such as we are now seeing between the U.S. and Mexico under the Bush and Fox administrations.

Beyond our immediate neighbors, we should more closely cooperate with our allies—the Europeans in particular. Their intelligence services are also collecting information on persons who may be a potential threat or have engaged in criminal activity. Consistent with the need to protect the privacy of innocent persons, we should have some access to their version of the lookout list, and reciprocate by sharing what we know about individuals who may be dangerous.

Sharing Passenger Lists. Airlines know in advance who will be flying to the U.S. through their reservation system. As travelers prepare to board a plane, they must identify themselves to the airline. Requiring all airlines to submit this information would give U.S. authorities an opportunity to compare the passenger list to their lookout lists. In this way, those who should not be permitted to enter the U.S., or those who are wanted for criminal activity can be prevented from entering, or apprehended while attempting to enter or leave.

Monitoring Individuals Once In the U.S.

Exit/Entry Systems. Every individual who comes into a U.S. airport must be inspected by immigration officers, where the entry is recorded. Airlines collect a boarding pass from the person as he or she departs

the U.S. Some airlines, but not all, have automated the collection of information from the boarding pass and forward the information to the U.S. government. When the government receives information on persons leaving the U.S., it can compare the information with those who have entered, and determine whether a person is leaving within the time allowed by his or her visa.

This “entry/exit” information system was supposed to be implemented at all airports. Implementation, however, has been left to the *voluntary* compliance of airlines. Not all airlines have cooperated, in part because the system requires an investment in equipment for a security function that, it might be argued, is not properly the role of private companies to fund. The funding and implementation of such a system to collect information on departing passengers for all of our airports and for all airlines should be provided by the federal government.

Entry and exit information would give authorities information on whether a person left within his visa timeframe. It would *not* tell authorities why a person did not depart in time, nor would it tell authorities where to find the person. It would not distinguish between someone staying an extra week to take care of a sick relative and someone plotting a terrorist act. The information might be useful where law enforcement officials develop an interest in an individual after the person entered the U.S. (for example, in the case of an individual who has been placed on the lookout list *after* being issued a visa). Authorities would then have a record as to whether the individual entered the country, and whether he departed.

An entry/exit information system has been discussed for land border points of entry into the U.S. as well. Such a system would be much more difficult to implement, would potentially be extremely disruptive to commerce with our largest trading partners, and would likely contribute little to the security of the U.S. Instead, a partnership with Mexico and Canada in carefully scrutinizing those flying to North America would be more effective in screening out persons who might potentially harm our country.

Monitoring Foreign Students and Trainees. Each year, hundreds of thousands of foreign students are admitted to the U.S. Certain conditions are attached to the student visa. For example, students are supposed to be enrolled in a certain amount of coursework. If they fail to maintain the conditions of their visa, the educational institution is supposed to inform the INS. Over the last several years, the INS has been working with colleges and universities to develop a system to collect information electronically, in a timely manner, on the status of foreign students. Currently, the system is only beginning to be implemented, as an operational prototype in few educational institutions. (Other institutions are required to collect the same information about a student’s status, but except for the limited prototype, the system is manual.) Funding could be provided by Congress to get the system, called the Student and Exchange Visitor Information System, up and running in all schools authorized to enroll foreign students. The system requires reporting on the identity and current address of the student or trainee, the academic status of the student, the degree program and field of study, practical training, beginning and ending dates, termination dates and reasons for termination, the number of credits completed per year, and other information.

However, as with the exit/entry system, even if such a system were in place it would only be able to tell authorities whether the student was properly maintaining status. It would not necessarily help authorities locate an individual who violated his visa terms. As the prototype is expanded, the INS should assess and report to Congress the feasibility of this system, and whether it can measurably improve the security of the U.S. relative to the cost of implementation, and do so in a way that does not excessively intrude on the privacy rights and civil liberties of students.

Monitoring Foreign Workers. Just as schools are required to report on the status of their foreign students, companies who employ foreign workers on temporary visas could be required to report on the

status of those workers. The various types of temporary visas granted to foreign workers have certain conditions that must be met, as well as time limits. Information provided by companies that hire these individuals—whether the person who was issued the visa has shown up for work, has completed the term of the visa, or has left the employer’s workforce—would be useful in determining whether these workers are complying with the terms of their visas. As with the student monitoring system, the benefits of such a system might not outweigh the cost of implementation or the concerns about potential violations of privacy and civil liberties.

Monitoring Schools with Foreign Students. Currently, there are approximately 74,000 schools authorized by the INS to enroll foreign students. Once a school obtains permission from the INS to enroll foreign students, there is very little monitoring of that school. The government might consider more closely monitoring schools, to ensure they are complying with the obligations they must meet to enroll foreign students.

Stricter Laws Governing Document Fraud. Currently, counterfeit identification documents can be easily bought from companies that manufacture them and advertise their sale. We may need to examine our laws regarding the selling of fraudulent documents, to close loopholes and increase punishment.