Statement by Assistant Secretary of State for Consular Affairs
Maura Harty
Before the House Committee on Government Reform
"A Look at the Goals and Challenges of the US-VISIT Program"
March 4, 2004

Mr. Chairman and Members of the Committee:

Thank you for inviting me to testify before you today on the Bureau of Consular Affairs' Visa Biometric Program and our role in implementing Section 303 of the Enhanced Border Security and Visa Entry Reform Act. The Department of State's visa work abroad constitutes a vital element in providing for our national border security. We have no higher responsibility than the protection of our citizens and safeguarding our country's borders through the visa process. The consular officers of the Foreign Service who adjudicate visas at our embassies and consulates abroad are truly our first line of defense. Through them, our goal is to push the very borders of the United States out as far from our shores as possible to stop a problematic or questionable traveler overseas. The Biometric Visa Program allows us to do just that by enhancing the integrity of the visa process and by helping consular officers identify visa applicants already known to U.S. law enforcement.

As you know, Section 303 of the Enhanced Border Security and Visa Entry Reform Act requires that no later than October 26, 2004, the Secretary of State issue to aliens only visas that use biometric identifiers. To comply with this requirement with respect to nonimmigrant visas, the State Department began deployment of the Biometric Visa Program on September 22, 2003. I am pleased to report that the program is now operational at more than 80 visa-adjudicating posts. The program will be in effect at all visa-adjudicating posts by October 26 of this year. We also began issuing biometric immigrant visas last month and will have this program operational at all immigrant visa-adjudicating posts by the same date.

Our Biometric Visa Program complements and reinforces the Department of Homeland Security's US-VISIT Program, which tracks the entry and exit of foreign visitors by using electronically scanned fingerprints and photographs. Together this system, which begins with consular offices collecting electronically scanned fingerprints at consular sections abroad and continues with DHS's US-VISIT program at ports of entry and departure, will create a coordinated and interlocking network of border security in which the American people can have confidence.

Consular officers abroad oversee the fingerprint enrollment of the visa applicants with fingerprint scanners at the visa interview windows. Enrollment time averages about 30 seconds. As soon as the fingerprints are enrolled they are sent electronically, along with the photo of the applicant and biographic data, to the Consular Consolidated Database (CCD) in Washington. The CCD relays the fingerprint files to DHS's IDENT system over a reliable, direct transmission line, which sends the results back to the CCD for relay back to the post. To date, seven pilot posts (Sanaa, Riyadh, Kuwait City,

Jeddah, San Salvador, Hong Kong, and Recife) are checking against the IDENT database and we are bringing the others on-line as quickly as possible. For those pilot posts, no visa can be issued until a response of no derogatory information found is returned from the IDENT system. Until such information from IDENT is received, the visa system is locked with regards to that visa application. For the remaining posts, the IDENT checks are being reviewed in the Department and posts are notified of any hits.

If the fingerprints match fingerprints provided by the FBI in the IDENT lookout database, the IDENT system returns to the post an FBI file number. At present, Consular officers have no easy access to the FBI record associated with that file number. As an interim procedure, we are processing such cases through our National Visa Center, where an FBI official receives and analyzes the FBI's records and then forwards the information to post. We are discussing means to enhance the efficiency of the process with the FBI, so that consular officers in the field will have more direct access to National Crime Information Center (NCIC) information that will be of use in adjudicating the visa to conclusion.

If there is no match against the IDENT lookout database, then the visa applicant's fingerprints are stored in the US-VISIT database in IDENT, and a fingerprint identification number (FIN) is returned to the post. Once the visa has been issued, our nonimmigrant visa system sends to the DHS Interagency Border Inspection System (IBIS) the issued visa data, including the visa applicant's photo and the fingerprint identification number. When the visa applicant arrives at a port of entry, the US-VISIT system will use the fingerprint identification number to match the visa with the file in IDENT, and will compare the visa holder's fingerprints with those on file. This one-to-one fingerprint comparison ensures that the person presenting the visa at the port of entry is the same person to whom the visa was issued.

Since we have only recently begun to incorporate biometrics into the U.S. visa adjudicating process, we have taken steps to ensure the continued integrity of those visas issued without biometrics. There are currently some 20 million valid nonimmigrant visas that are not biometric visas. To ensure the integrity of these valid visas that do not have associated biometric data captured at visa issuance, we have upgraded our visa datashare program for use at primary inspection under US-VISIT. Under visa datashare, the biographic data and photo from the issued nonimmigrant visa are stored on the IBIS computer. When the DHS officer scans the visa at primary inspection, the photo and biographic data of the applicant are extracted from the database and projected on the screen. If the traveler has altered the photo on the visa, the DHS officer will be able to make a comparison with the original photo. In one such case under US-VISIT, a woman's photo appeared on the screen, but the traveler presenting the visa was a man. If the visa is a complete counterfeit, nothing will appear on the DHS officer's screen. In this way, US-VISIT is combating fraud and protecting the integrity of the U.S. visa. The process for the biometric immigrant visa will be very similar. The visa itself will be printed on a tamper-resistant document. There will be reliable datashare with DHS so that the DHS inspector at the port of entry can verify the identity of the traveler and the authenticity of that individual's status as a new immigrant.

Just as we are committed to the most secure adjudication process and documentation to support the visa process, the same is true in terms of what I consider to be the world's most valuable document--the U.S. passport. The legislative requirements of the Border Security Act apply only to passports issued by Visa Waiver Program (VWP) countries, but not the U.S. passport. We recognize that convincing other nations to improve their passport requires U.S. leadership both at the International Civil Aviation Organization (ICAO) and by taking such steps with the U.S. passport. Embedding biometrics into U.S. passports to establish a clear link between the person issued the passport and the user is an important step forward in the international effort to strengthen border security. To this end, we are introducing "contactless chips" into U.S. passports, electronic chips on which we will write the bearer's biographic information and photograph. Our program should produce the first biometric U.S. passports using ICAO's standard of facial recognition in October of this year and complete the transition to biometric passport by the end of 2005.

The Border Security Act also established October 26, 2004, as the date by which VWP countries must issue to their nationals only machine-readable passports (MRP) incorporating biometric identifiers that comply with the standards established by ICAO. ICAO's decision to make facial recognition technology the standard passport biometric was not made until May 2003, leaving VWP countries only 17 months to bring a biometric passport from design to production, a process that normally takes years. Very few, and potentially no, VWP countries will be able to meet the legislatively mandated deadline by which to issue to their nationals only machine-readable passports (MRP) incorporating biometric identifiers that comply with the standards established by the ICAO. Although the VWP country governments share a commitment to make this change, many of them are encountering the same problems being experienced by the Department of State in our effort to introduce embedded biometrics into the U.S. passport. These issues include ICAO resolution on security matters, interoperability of readers and passports, procurement and chip supply difficulties, as well as comprehensive testing to ensure that the chips work successfully and that they will continue to do so through the validity of the passport, which is 10 years in most cases.

We have vigorously encouraged VWP countries to issue biometric passports by the October 26, 2004, deadline. The U.S. has played a leadership role in ICAO working groups to advocate the successful inclusion of biometrics in travel documents. In the G8 we strongly advocated support for ICAO leadership in biometrics and participated fully in a special working group on biometrics established by the G8 ministers of Home and Justice Affairs. We are fully engaged in the group of 5 (US, UK, New Zealand, Australia, Canada) in which there are continuing discussions on progress reports on each country's efforts to produce the passport. On the margins of international conferences, we have had repeated meetings with VWP representatives to explain the process; at trade conferences, State Department officials have made many public appearances to educate VWP government representatives about the requirements and deadlines. Many VWP countries have sent representatives to Washington to meet with U.S. government representatives and had full and open discussions on the issue. In testament to our

efforts, all VWP countries are making varying degrees of progress toward complying with the biometric requirement. Despite our efforts, however, almost none will meet the October 26, 2004, deadline. None of the larger countries (Japan, the U.K., France, Germany, Ireland, Italy or Spain, for example) will begin issuing passports with biometrics by October 26. Japan and the United Kingdom say they will begin in late 2005; others may not come on-line until a year after that.

Since travelers from VWP countries with passports issued on or after October 26, 2004, that do not contain biometrics will need visas to travel to the U.S., we estimate that the demand for nonimmigrant visas will jump by over five million applications in FY 2005, nearly double last year's workload. Biometrically enhanced passports will add to border security, and we are heartened by the commitment by these countries to developing the passports as quickly as possible and by their progress to date.

The inclusion of biometrics in international travel documents is an important step in continuing to improve our ability to verify the identity of prospective travelers to the United States, especially individuals who might be terrorists, criminals, or other aliens who present a security risk to the United States. The Department of State is working hand in hand with our colleagues at the Department of Homeland Security to ensure that we have a system that facilitates legitimate international travelers and properly identifies those who pose a threat to prevent them from entering our country. The continued commitment to ensuring the sanctity and security of our borders and our nation is the number one priority. I am happy to answer any questions you may have.