Statement by Assistant Secretary of State for Consular Affairs
Maura Harty
Before the House Select Committee on Homeland Security,
Subcommittee on Infrastructure and Border Security
January 28, 2004

Mr. Chairman and Members of the Committee:

Thank you for inviting me to testify before you today on the role of the Bureau of Consular Affairs in implementing Section 303 of the Enhanced Border Security and Visa Entry Reform Act (Border Security Act). The inclusion of biometrics, in addition to the photograph that has always been collected, 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. In the process of screening visas and passports domestically and abroad, additional biometrics can serve as a useful adjunct to existing screening processes that identify individuals who might be terrorists, criminals, or other aliens who might represent a security risk to the United States. The Department of State has invested substantial time, money, and effort to implement the additional biometrics and ensure that international visitors are aware of changes to the visa application process and admission procedures in the United States. In so doing, we have worked, and will continue to work, closely with our colleagues at the Departments of Homeland Security and Justice (including the FBI).

As you know, the Border Security 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, at the U.S. Embassy in Brussels, Belgium, and quickly followed suit at the U.S. Consulate General in Frankfurt and Embassies in San Salvador and Guatemala City. I am pleased to report that the program is now operational at 55 visa-issuing posts and with our aggressive rollout schedule the program will be in effect at all visa-issuing posts by October 26 of this year. With regard to immigrant visas, we will start issuing biometric visas in February and have this program operational at all immigrant visa-issuing posts by October 26, 2004.

The success we are having with the rollout of the Biometric Visa Program should not detract from the accomplishments of the process itself. I would like to walk you through the nonimmigrant visa process from visa applicant enrollment to the traveler's arrival at the U.S. port of entry.

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 in Rockville over a reliable, direct transmission line, which sends the results back to the CCD for relay back to the post. The current return time is approximately seven to eight minutes at three 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 regard to that visa application. 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 at posts overseas do not have desktop 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.

As I mentioned before, biometrics (including photos and fingerprints) are a useful adjunct to the existing screening procedures. Even though fingerprint data has only recently begun to be incorporated into the U.S. visa issuing process, through our visa datashare program, which has been upgraded for use at primary inspection under US-VISIT, we are able to ensure the integrity of valid visas that do not have associated fingerprint data captured at visa issuance.

I will quickly outline the process by which visa datashare helps us accomplish our goal of securing further the integrity of the U.S. visa. Under visa datashare, the biographic data and current biometric data (i.e. 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. At the same time, this system facilitates travel for the legitimate traveler because the DHS officer need not spend time examining the visa to ensure its authenticity – the US-VISIT system is ensuring the visa authenticity.

The process for the biometric immigrant visa that includes a fingerprint 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.

Let me now turn to the issue of the U.S. passport, which I firmly believe is the world's most valuable identity and travel document. First, I think it is important to note that improving passport security is not a one-time effort. Instead, we are involved in a process of continuous improvement that affects not just the physical passport carried by an American citizen, but also the adjudication process that determines whether an applicant is in fact a U.S. citizen.

Our latest efforts to improve the U.S. passport began in the late 1990's with the introduction of photodigitization technology to support passport printing. Instead of gluing a physical photograph of the applicant into a passport and protecting that photo with a laminate, we introduced an entirely new technique that takes advantage of the many improvements in digital technology during the last decade. Photodigitization has been an unqualified success. Any passport with a physical photograph is inherently susceptible to photo substitution. We have now produced over 25 million passports using photodigitization and the number of credible alterations we have encountered still number in the single digits. I should add that domestic photodigitization has been so successful that we have, in turn, returned the production of passports issued abroad to our U.S. domestic production facilities so that we can take advantage of the significant security improvements embodied in the photodigitization process.

But, as good as photodigitization is, it is not the end of our efforts. We are currently undertaking a total redesign of our passport book to introduce the latest generation of security features as well as a total update of the physical appearance of the inside of the book. More significantly, we are also undertaking a massive effort to introduce embedded biometrics into the U.S. passport through the insertion of a contact-less chip, which will store biometric and biographic data including digital photos. I think it is important to note, however, that the legislative requirements in that section do not apply to U.S. passports, only to passports issued by our partner nations in the Visa Waiver Program.

Embedding enhanced biometrics into passports so that a clear link can be established between the authorized bearer of that passport and the user is an important step forward in the international effort to strengthen border security. We recognize that convincing other nations to change and improve their passport requires U.S. leadership both at the International Civil Aviation Organization (ICAO) and practically by introducing these changes into the U.S. passport. Thus, the Department of State has underway a program that should result in the production of our first enhanced biometric passports using the ICAO standard of facial recognition techniques in October of this year and we plan to complete the transition to this new biometric passport by the end of calendar year 2005.

In addition to our enhanced biometric initiatives, we are moving forward aggressively on two other programs to further improve further the U.S. passport. The first of those programs is to redesign the passport itself. We are well advanced on this project and expect to have these new

books in large-scale production later this year. We have also implemented and expanded our data base which immediately alerts ports of entry to any passports reported lost or stolen.

The second is to strengthen further our passport adjudication process. We are negotiating new datasharing agreements with agencies such as the Social Security Administration (SSA) so that we can gain access to SSA data, which when combined with data from other sources, will help to identify possible irregularities in passport applications. We are also receiving additional data from the law enforcement community to help prevent issuance of passports to persons who may be flight risks. We are examining the possible uses of decision based software techniques and commercial database searches as part of a longer range effort to give passport adjudicators every possible tool to ensure the accuracy of their decisions. We will complete the scanning of applications with images for all currently valid passports by April, making them available at the desktop level worldwide to assist in adjudication. Finally, we should soon sign an agreement with DHS that will allow border inspectors access to these electronic copies of passport applications as a way to help strengthen our processing systems for returning American citizens.

Now that I have addressed the accomplishments that we are making towards improving the biometrics currently in our passports, I would like to focus on other countries efforts towards the same end. The Border Security Act set October 26, 2004 as the date when VWP travelers with passports issued on or after that date must also have biometrics (digital photos) incorporated in those passports that meet the ICAO standard for use in visa-free travel to the United States. Visa Waiver Program (VWP) governments have indicated that they will be unable to meet the legislatively mandated deadline to issue to their nationals only machine-readable passports (MRP) incorporating this enhanced biometric identifier that complies with the standards established by the ICAO.

ICAO's decision to make facial recognition technology the standard passport biometric was not made until May, 2003, leaving countries only 17 months to bring a biometric passport that meets that standard from design to production, a process that normally takes years.

Moreover, while 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 enhanced biometrics into the U.S. passport. These issues include needing final decisions through the ICAO process on security matters, resolution of interoperability matters, 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 that meet the ICAO standard 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 regarding 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 December, the Secretary of State sent a diplomatic note to the VWP Embassies in Washington that conveyed the criteria for certification of a biometric passport program and also noted that there is no waiver available for the production deadline. The State Department followed up by sending the text of the note to U.S. Embassies in the VWP countries and requested the Embassies deliver the information to the host government and have them reply by January 10. We are still receiving responses from those countries.

In testament to our efforts, all VWP countries are making varying degrees of progress toward complying with the requirement to have a program in place to issue biometric passports; however, only one or two countries may have production capability in place by October 26, 2004. None of the larger countries (Japan, the U.K., France, Germany, Ireland, Italy or Spain, for example) will begin issuing passports with the ICAO biometric by October 26, 2004. 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 non-biometric passports issued on or after October 26, 2004 will need visas to travel to the U.S., we estimate that the demand for nonimmigrant visas will increase significantly over FY2005 to over five million applications, nearly double last year's workload. However, once VWP countries begin issuing passports with biometrics, the increased workload will disappear. For example, in FY 2003, mission Japan (Tokyo, Osaka, Kobe and Naha) processed approximately 111,000 nonimmigrant visa cases. The Japanese estimate that between October 26, 2004, and the introduction of their biometrics-bearing passport projected for November 2005, between 1.2 to 1.5 million Japanese would need visas. In FY 2006, the number would likely drop back to current levels.

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 continues to facilitate legitimate international travelers and properly identifies those who pose a threat to prevent them from entering our country. I think I speak for all of us here today when I say that 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. Thank you very much.