STATEMENT OF RICHARD L. SKINNER

ACTING INSPECTOR GENERAL

U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

SUBCOMMITTEE ON IMMIGRATION, BORDER SECURITY, AND CLAIMS

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

APRIL 21, 2005

Thank you, Mr. Chairman and members of the Subcommittee:

I'm pleased to have this opportunity to appear before you today to discuss the findings of our December 2004 review of the use of stolen passports from Visa Waiver countries to enter the United States and the threat that stolen Visa Waiver Program (VWP) passports pose to that program. More broadly, this is a threat posed to our national security as well. Copies of the report have been provided to the Subcommittee and are available to the public on our website.[1]

What did we inspect?

The VWP began in 1986. It enables most citizens from 27 countries to travel to the United States for tourism or business purposes for 90 days or less without obtaining a visa. From the beginning, the program involved a balancing of security risks and benefits to commerce, tourism, foreign relations, and the workload of the Department of State. In late 2003 and early 2004 we studied the security implications of the visa waiver program and released a report in April 2004. Copies of that report also have been provided to the Subcommittee and are available to the public on our website.[2]

Virtually all those familiar with the Visa Waiver Program told us at that time that the lost and stolen passport problem is the greatest security vulnerability associated with it. During the course of our VWP review we obtained documents that recorded instances in which blank, bona fide passports from VWP countries were stolen and, as determined from their serial numbers, later used to enter the United States, sometimes on multiple occasions. In some instances, entry was permitted even after the stolen passport had been posted in the lookout system. We therefore began a subsequent inspection of the specific problem posed by stolen VWP passports and issued a report in late December 2004.

What did the data show?

We examined all reported stolen passports from six VWP countries - France, Spain, Germany, Portugal, Belgium, and Italy - for a 5-year period – February 10, 1998, to February 12, 2003. There were 3,987 reported passports stolen; some were presented 176 times at Ports of Entry (POE).

Aliens applying for admission to the United States using stolen passports had little reason to fear being caught and usually were admitted, even if the stolen passport had been posted previously to CBP's lookout systems. Also, when DHS received new reports of stolen passports, it listed the passport number into its lookout system for future protection but did not check to determine whether a traveler had already used any of the newly reported passports. Finally, the Department of Homeland Security (DHS) did not have a sound procedure to ensure that when CBP records show a successful entry using a stolen

[1] "A Review of the Use of Stolen Passports from Visa Waiver Countries to Enter the United States" (OIG-05-07) December 2004.
[2] "An Evaluation of the Security Implications of the Visa Waiver Program" (OIG-04-26) April 2004.

passport, the event is referred to Immigration and Customs Enforcement (ICE) investigators to seek out and apprehend the user.

It made little difference whether the passport had been listed in a CBP lookout or not. Travelers using stolen passports, which had not been posted to the lookout, were admitted 81% of the time; travelers using stolen passports that had been posted to the lookout were admitted 73% of the time.

With respect to travelers whose passports had already been posted to a lookout as stolen, half were referred to "secondary inspection" for a more thorough examination. However, most referrals were for other reasons. The use of a stolen passport was not a recorded basis for the referral. Thus, after examination in secondary, half of the travelers were permitted entry. Some passports were used successfully multiple times to enter, despite being posted on the lookout system. We could not determine the inspectors' rationale for admitting the aliens with lookouts for the stolen passports. The records of the secondary inspections often were nonexistent or so sketchy that they were not useful.

Of the admissions on stolen passports, 33 occurred after September 11, 2001. Most disturbing, some passports that were used successfully came from blocks of stolen passports, which were associated with events or locations possibly linked to Al Qaeda.

DHS did not have a process to check lost and stolen passport information against entry and exit information. Upon receipt of a new report that passports have been stolen, CBP did not check to determine whether they have been used to enter the United States, nor did it have formal procedures to notify ICE of the use of a stolen passport so that an effort may be initiated to apprehend the traveler.

<u>We recommended that CBP:</u>

1. Require inspectors to refer aliens to secondary inspections when the passports are the subjects of lookouts;

2. Require that inspectors record in detail the results of the secondary inspections and justifications for subsequent admissions;

3. Require that a supervisor review and approve an inspector's decision to admit an alien who was the subject of a lookout, and that the review be recorded as part of the secondary inspections record;

4. Initiate routine reviews of admission records to identify prior uses of stolen passports; and,

5. Report information on the successful use of stolen passports to enter the United States to ICE for investigation.

We recommended that ICE:

1. Develop procedures to investigate, locate, and remove from the United States persons that have used stolen passports to gain entry to the country and to report the outcomes of its investigations to CBP; and,

2. Investigate the activities while in the United States of the aliens that used certain stolen passports and determine their current whereabouts.

CBP and ICE concurred with all of our recommendations and plan appropriate corrective actions. While our office believes that these actions have been undertaken, we have not performed any formal compliance review.

One concern noted in our report is international in scope, and will require an international solution, i.e., the ill-defined process by which each country's stolen and lost passport information is reported and disseminated among all the other countries. The department's information about stolen passports is often incomplete. It's our understanding that INTERPOL plans to expand and regularize the reporting of lost and stolen passports. This initiative, when fully implemented with all nations participating, should permit automatic checking at the port of entry to determine whether the traveler is presenting a lost or stolen passport.

Even with the completion of the corrective action we recommended, the VWP will always pose some security risk. The fundamental premise of the program is that millions of persons, about whom we know little, can be exempted from DOS' ever more rigorous visa procedures and permitted to board U.S.-bound planes. As we said in our report, "The visa is more than a mere stamp in a passport. It is the end result of a rigorous screening process the bearer must undergo before travel." By the end of the visa interview DOS has collected and stored considerable information about the traveler and the traveler's planned journey. DOS has introduced biometric features into its visas, shares data from its visa records with DHS port of entry systems, and significantly increased the percentage of applicants subject to a careful interview. In contrast, the visa waiver traveler is interviewed briefly, and the passport examined, again briefly by an inspector who may be unfamiliar with even valid passports from the issuing country.

One of the most significant corrective actions responsive to the concerns stated in our report is the processing of visa waiver travelers through U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT). As implemented in December 2003, US-VISIT excluded visa waiver travelers from its scope. We strongly recommended that visa waiver travelers be added to the US-VISIT program because of the additional screening, identification, and exit control features it offers. On April 21, 2004, DHS Secretary Ridge announced that BTS would begin to process visa waiver travelers through US-VISIT by September 30, 2004.

This brings me to another pressing border security matter much in the news recently – our land borders.

US-VISIT at the Borders

In February 2005 we released our inspection report on the implementation of US-VISIT at land border ports of entry.[3] The report was written because legislation mandated the implementation of an automated, integrated entry exit system at the 50 highest volume land ports of entry by December 31, 2004. We reviewed efforts undertaken by the US-VISIT Program Office to meet this deadline, develop implementation and deployment plans, modify existing facilities, conduct or plan pilot testing of systems and new technology, and achieve program goals.

The examination of entering travelers at land POEs presents special problems. For one, CBP officers do not have an opportunity to prescreen using aircraft and ship passenger manifests. At land POEs there is less use of automation to check watch lists and other databases as part of the screening process. Indeed, name checks are not run at all on the vast majority of entrants. At present, travelers entering the United States at a land Port of Entry are only processed through US-VISIT if they enter on the basis of a visa. This is a very small percentage of travelers. The US-VISIT enrollment at land ports of entry will include approximately 2.7 % of the foreign visitor population. Why is this percentage so small? There are several reasons.

Mexican Border Crossing Card (BCC) holders entering the United States are not likely to have their entry electronically captured, nor their identity verified. Most BCC cards are visually inspected by Customs and Border Protection (CBP) officers, not scanned at primary inspection. As a result, the BCC holder's identity is not verified nor the entry electronically recorded. BCC holders accounted for nearly 43.8% of foreign national land border crossings in FY 2002.

Visa exempt Canadians, who represent approximately 22% of foreign national land border crossings in FY 2002, are also exempt from US-VISIT enrollment. They are able to gain admission to the United States by providing documents with limited information to verify their identities. The procedure is similar to that for BCC entrants – visa-exempt Canadians are not likely to have their entry recorded, or their name checked against any watch list.

Lawful permanent residents (holders of green cards) represent 32 % of all foreign entrants. It is not standard procedure at a land POE to screen their names or record their entries.

Together all of these categories of foreign entrants represent two-thirds of the total at the land POEs; the other third are American citizens. American names are not screened against watch lists, and their entries are not recorded. The problem for border security is the possibility that someone is posing as an American, who is not an American.

[3] "Implementation of the United States Visitor and Immigrant Status Indicator Technology Program at Land Border Ports of Entry" (OIG-05-11) February 2005.

Detection of such imposters is weakened by the absence of automated and biometric checks.

Thus, while US-VISIT offers potential, few travelers are actually covered. Moreover, while US-VISIT may have met minimum statutory requirements for implementation at land borders, it lacks the exit component necessary to identify those who overstay the terms of their admission.

In addition, when trying to establish an individual's identity and determine admissibility, CBP officers currently perform queries of multiple information technology systems, many of which employ old technology and cannot interface. Achieving system integration becomes particularly important at land ports because inspection time is limited and there is no advance passenger information.

Fully implementing a comprehensive solution of integrated systems, processes, and data for electronically tracking the pre-entry, entry, status management, and exit of all classes of foreign national visitors seeking admission to the United States will be a complex, technologically challenging, and expensive project that will not be realized for at least five to ten years.

Current Initiatives

The recently enacted Intelligence Reform and Terrorism Prevention Act of 2004 requires that, by January 1, 2008, all travelers must provide evidence to establish identity and citizenship when entering the United States. Specifically, it requires that DHS develop and implement, as expeditiously as possible, a plan that requires a passport or other document, or combination of documents that sufficiently denotes the identity and citizenship for all travelers entering the United States. This includes not only those categories of individuals for whom documentation requirements had been waived previously but also U.S. citizens.

This represents a bold step towards exercising better control of our borders. As the GAO clearly documented in its unclassified testimony GAO-03-713T "Counterfeit Documents Used to Enter the United States From Certain Western Hemisphere Countries Not Detected", and its Limited Official Use report GAO-03-782 "Land Border Ports of Entry: Vulnerabilities and Inefficiencies in the Inspections Process", our land borders are easily breached by imposters with phony birth certificates and driver's licenses.

The dialogue over how to improve document integrity, to track arrivals and departures, to employ biometric identifiers, which biometric identifiers to rely on, and how to automate screening transactions will continue. So will our office's monitoring of these very important programs.

Mr. Chairman, this concludes my remarks. I will be pleased to answer any questions the Subcommittee may have.