

**DEPARTMENT OF HOMELAND SECURITY**  
**Office of Inspector General**

**An Evaluation of the Security  
Implications of the  
Visa Waiver Program**



Office of Inspections, Evaluations, & Special Reviews

OIG-04-26

April 2004



## Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, investigative, and special reports prepared by the OIG periodically as part of its oversight responsibility with respect to DHS to identify and prevent fraud, waste, abuse, and mismanagement.

This report is the result of an assessment of the strengths and weaknesses of the program, operation, or function under review. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, and a review of applicable documents.

The recommendations herein have been developed on the basis of the best knowledge available to the OIG, and have been discussed in draft with those responsible for implementation. It is my hope that this report will result in more effective, efficient, and/or economical operations. I express my appreciation to all of those who contributed to the preparation of this report.

Clark Kent Ervin  
Inspector General



# Contents

---

Introduction.....	3
Results in Brief .....	3
Background.....	5
Purpose, Scope, and Methodology.....	7
The Visa Waiver Program in Perspective.....	7
VWP Management.....	10
VWP Overstay Reporting.....	11
VWP Country Reviews.....	13
Lost and Stolen Passports.....	15
Reporting LASP Information.....	16
Detection of Stolen VWP Passports.....	17
Stolen Passports Returned to Travelers.....	20
US-VISIT and VWP .....	21
Biometric Passport Deadline.....	23
POE Inspector Training.....	24

## Appendices

Appendix 1: Countries in the Visa Waiver Program.....	26
Appendix 2: Nonimmigrant Admissions for VWP Countries, 1998 - 2003 .....	27

# Contents

---

Appendix 3:	Nonimmigrant Visa Issuances in VWP Countries Before and After VWP Accession.....	28
Appendix 4:	Legislative History of the Visa Waiver Program .....	30
Appendix 5:	Management Comments .....	36
Appendix 6:	OIG Evaluation of Management Comments.....	37
Appendix 7:	Recommendations.....	38
Appendix 8:	Major Contributors to this Report.....	40
Appendix 9:	Report Distribution .....	41

## Abbreviations

APIS	Advance Passenger Information System
BTS	Border and Transportation Security Directorate
CBP	Bureau for Customs and Border Protection
CCD	Department of State’s Consular Consolidated Database
CLASS	Consular Lookout and Support System
DHS	Department of Homeland Security
DMIA	2000 INS Data Management Improvement Act
EBSVERA	2002 Enhanced Border Security and Visa Entry Reform Act
FDL	Forensic Documents Laboratory
FY	Fiscal Year
GAO	Government Accounting Office
ICAO	United Nations International Civil Aviation Organization
ICE	Bureau for Immigration and Customs Enforcement
ICN	Inventory Control Number (of a passport book)
IIRIRA	1996 Illegal Immigration Reform and Immigrant Responsibility Act
IMMACT	1990 Immigration Act
INA	1952 Immigration and Nationality Act
INS	Immigration and Naturalization Service
IRCA	1986 Immigration Reform and Control Act
LASP	Lost and Stolen Passports
MRP	Machine-Readable Passport
MRV	Machine-Readable Visa
OIG	Office of Inspector General
POE	Port of Entry
TECS	Treasury Enforcement Communications System

# Contents

---

TIPOFF	Department of State Terrorist Information Watchlist
USA PATRIOT Act	2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
US-VISIT	US Visitor and Immigrant Status Indicator Technology
VWP	Visa Waiver Program
VWPP	Visa Waiver Pilot Program
VWPPA	2000 Visa Waiver Permanent Program Act

# OIG

---

## *Department of Homeland Security Office of Inspector General*

### **Introduction**

We evaluated the Border and Transportation Security directorate's (BTS) management of the Visa Waiver Program (VWP).<sup>1</sup> The VWP was first established as a pilot program in 1986. By 1989, the Attorney General and the Secretary of State designated eight countries to participate in the program. As of March 2004, there were 27 designated VWP participating countries.<sup>2</sup>

The VWP enables citizens of certain countries to travel to the United States for tourism or business for 90 days or less without obtaining a visa. The Visa Waiver Permanent Program Act (VWPPA)<sup>3</sup> was approved in 2000. The Homeland Security Act of 2002 vested in the Secretary of Homeland Security "all authorities" to issue regulations, to administer, and to enforce all immigration and nationality laws.<sup>4</sup> (A legislative history of the VWP is at Appendix 4.)

Prior to the establishment of DHS, the Department of Justice (DOJ) Office of the Inspector General (OIG) examined VWP operations in 1999 and 2001. DOJ OIG identified several chronic and recurring problems and made a series of recommendations to strengthen implementation of the program. The General Accounting Office (GAO) also issued a report<sup>5</sup> in November 2002 assessing VWP operations, but did not address the VWP's security aspects.

In this report, we examined BTS' management of the VWP, focusing on security issues that could threaten the safety and security of the United States.

### **Results in Brief**

Since 1988, several hundred million visitors have entered the United States as VWP travelers resulting in convenience and savings to foreign travelers, substantial economic benefits to the United States, reduced costs for U.S. visa and

---

<sup>1</sup>Immigration and Nationality Act (8 U.S.C. 1187), Sec. 217.

<sup>2</sup> List of designated VWP participating countries is at Appendix 1.

<sup>3</sup> P.L. 106-396.

<sup>4</sup> P.L. 107-296, Sec. 428.

<sup>5</sup> GAO-03-38



---

entry processing, and reciprocal visa-free travel for Americans to VWP designated countries. After 12 years of pilot operations, Congress recognized these benefits and made the VWP a permanent program in 2000. Congress strengthened provisions of the VWP to ensure that the program did not adversely affect the law enforcement and security interests of the United States.

We identified significant areas where BTS needs to strengthen and improve VWP performance. VWP organizational issues have not been fully resolved since the Department of Homeland Security (DHS) was established in March 2003. Since the dissolution of the Immigration and Naturalization Service (INS), the VWP has had a series of acting managers and officials sharing responsibilities. It is not clear to many within DHS or other federal agencies who is in charge of the VWP.

Due to a current lack of funding, trained personnel, and other issues, BTS is unable to comply with the mandate to conduct “country reviews” of each VWP-designated country every two years to determine whether that country shall be continued in the program. BTS has not developed a process, and does not have an approved inter-agency protocol, for conducting such reviews. On the immediate horizon, there is no process for determining whether to continue the designation of Belgium as a VWP country when its one year probationary status ends on May 15, 2004.

BTS’ lack of readiness to conduct VWP country reviews directly undercuts its ability to assess the most serious security problem inherent in this program--lost and stolen passports (LASP). LASP information provided by VWP governments has not been thoroughly checked by the former INS or now by BTS against U.S. entry and exit information to determine whether the passports have been used to enter the United States. Collection of LASP data from VWP governments is not proactive or uniform, nor is the data disseminated in an organized fashion. Further, LASP problems are complicated by the lack of international standardization in passport numbering systems that can result in a failure to identify *male fide* travelers using stolen VWP passports.

Finally, there are two other issues with security implications for the VWP: a potential security weakness in the fraudulent use of VWP passports to bypass the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) procedures; and inadequate training in passport fraud for inspectors at ports of entry (POEs).

---

We are recommending that BTS:

- 1) Designate a VWP program manager with clearly defined responsibilities and authorities;
- 2) Develop a plan to conduct the mandated VWP annual reports;
- 3) Develop protocols and a plan to conduct biennial country reviews;
- 4) Provide funding to support the conduct of the country reviews;
- 5) Develop a process for reviewing the probationary designation of Belgium, so that a decision can be rendered prior to May 15, 2004;
- 6) Develop a process comprehensively to check all lost and stolen passport (LASP) data provided by VWP governments against entry and exit data in U.S. systems;
- 7) Develop procedures to collect and analyze data concerning the fraudulent use of VWP passports;
- 8) Include in the country review protocols provisions to review document manufacturing and issuing security practices;
- 9) Coordinate with the Department of State to establish a standard operating procedure for the systematic and proactive collection of LASP information;
- 10) Require that inventory control numbers and passport numbers be queried in lookout systems;
- 11) Review current policies that allow the return of fraudulent travel documents to those who presented them when they are sent back to their countries of origin;
- 12) Require, as soon as US-VISIT capabilities permit, that VWP travelers be screened by US-VISIT procedures;
- 13) Develop and recommend legislation to grant DHS waiver authority for VWP countries that cannot comply with the biometric passport deadline; and
- 14) Provide additional training in passport fraud detection for POE inspectors.

On March 11, 2004, we sent a draft copy of this report to the Undersecretary for Border and Transportation Security and additional copies to various program managers and liaison points of contact within DHS. The draft report was sent for the purpose of obtaining comments or factual additions that the readers might have believed appropriate. The draft was also sent to obtain a response to our recommendations and an indication whether the component agreed to take corrective action. We asked for a response in 30 days from issuance of the draft report.

---

Although we allowed the component additional time to issue its response, none was received. Accordingly, we are issuing the final report without the benefit of the component's response.

Although we have not received a response from DHS to our draft report, several of our recommendations have been the subject of public commentary in recent weeks. On April 2, 2004, DHS announced that it will begin processing VWP passengers through US-VISIT by September 30, 2004 (see our recommendation number 12), and that it would seek an extension of time for the biometric passport deadline (see our recommendation number 13). Informally, we have learned that the requirements that DHS conduct country reviews may have received new attention and resources recently (see recommendation numbers 3 through 5). Because we have not received a reply from BTS responding formally to our recommendations and providing sufficient detail to show how corrective action will be accomplished, all 14 recommendations are unresolved at this time.

## Background

### **Procedural Differences Between Inspections of Visa and VWP Travelers**

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 process, U.S. authorities have collected and stored considerable information about the traveler and the traveler's planned journey. When the visa is waived for broad classes of travelers, those travelers avoid this extensive examination and the United States does not collect comparable information regarding them.

Visa applicants answer 40 questions when they complete the *Nonimmigrant Visa Application Form (DS-156)*. If male and between the ages of 16 and 45, they must answer 18 additional questions on the *Supplemental Nonimmigrant Visa Application Form (DS-157)*. Another supplemental form, the *Contact Information and Work History for Nonimmigrant Visa Applicant (DS-158)*, is sometimes used. These questions elicit detailed information from the applicants about their personal biography; their employment history; the purpose, duration, and destination of their planned travel; the immigration status of close family members; and their prior visa history. All of this information is used by the consular officer to decide whether to issue the visa, and if so, which type.

The Department of State computer system processes the visa applications and prints the visas. The system maintains an electronic record of the applicants'

---

photographs and their responses to many of the questions on the forms. In earlier years, much of the information submitted by the applicant was not entered into the computer, which originally was just a visa printing device. In 2003, the system's software was improved to collect and preserve additional data fields relevant to the alien's travel. The Department of State began collecting digital fingerprints of visa applicants in 2003. Some information about the traveler's visa application is stored in the Consular Consolidated Database (CCD). Some of the CCD information is available to inspectors at the POEs, who can use it to verify the arriving traveler's identity and the stated purpose of their travel. Upon arrival at the POE, a traveler with a visa will submit a completed *Form I-94, Nonimmigrant Arrival/Departure Form*, which contains 13 questions to identify the alien in the computerized arrival system.

In contrast, all a VWP traveler completes is *Form I-94W, Nonimmigrant Visa Waiver Arrival/Departure Form*. It asks for the traveler's name and date, but not place of birth; country of current, but not former, citizenship; country of residence; passport number, but no visa information; and a U.S. destination address. POE inspectors cannot use appointment systems to manage their workload. Hundreds, and sometimes thousands, of travelers can descend on them almost at once. While a previous requirement to clear all passengers from a flight within 45 minutes was abandoned following the terrorist attacks of September 11<sup>th</sup>, the managers at the POEs we visited still consider the 45-minute a goal to be achieved as often as possible.

POE inspectors told us that when they see a recently issued visa in a traveler's passport, and in the absence of indications of fraud, they are inclined to believe that the traveler is likely to be admissible. Some inspectors expressed envy at the tools available to consular officers: the language and other professional training, the experienced foreign staff knowledgeable about local fraud trends, and the time to conduct a thorough interview, requiring the applicant to come back again another day, if necessary, with supporting documents.

Consular officers usually receive training in the language spoken most commonly in the country to which they are assigned. This training enables them to communicate with the majority of the people that they encounter in their jobs. However, POE inspectors interview a diverse stream of passengers that speak many different languages. It is unlikely that POE inspectors can speak all of the languages encountered in their jobs. One interview we observed at a POE was illustrative of the language problem embassies do not face. The traveler, presumably Japanese, behaved as if he spoke no English. The inspector did not

---

speaking any Japanese and posed a series of questions in English to the traveler, who simply stared back. Eventually the inspector asked: “You’re a tourist, right?” while bobbing his own head up and down. The foreigner nodded his head, too, and was admitted without having spoken a word.

## **Purpose, Scope, and Methodology**

We conducted this evaluation to assess BTS’ management of the VWP, focusing on the program’s security aspects. Our goal was to examine VWP’s organization, policy requirements, and field operations comprehensively. Beginning in October 2003, the Office for Inspections, Evaluations, and Special Reviews conducted interviews and reviewed documents at DHS headquarters in Washington, D.C. We conducted interviews with DHS personnel from CBP, the Bureau of Immigration and Customs Enforcement (ICE), CBP’s National Targeting Center (NTC), BTS’ US-VISIT Office, and ICE’s Forensic Document Laboratory (FDL). Additionally, we conducted interviews with several analysts and advisors with prior experience in the VWP who are now working at the Central Intelligence Agency’s Terrorist Threat Integration Center and the Federal Bureau of Investigation’s Terrorist Screening Center. Information and documents were also collected from senior officials at the Department of State and the Department of Justice. We visited POEs at Washington Dulles, Miami International, Newark International, and John F. Kennedy International Airports, as well as land POEs at Peace Bridge and Rainbow Bridge in New York. Finally, we traveled to five VWP countries -- Belgium, France, United Kingdom, Singapore, and Brunei -- in order to observe U.S. visa operations and to consult with U.S. and foreign officials in those countries regarding the VWP.

## **The VWP in Perspective**

Hundreds of millions of travelers from VWP countries visited the United States since program operations began in 1988.<sup>6</sup> In the last five years alone, there have been 93 million nonimmigrant admissions from VWP countries.<sup>7</sup> The positive effects of such a large number of foreign visitors on the U.S. economy, particularly the tourism and commerce sectors, were significant.<sup>8</sup>

---

<sup>6</sup> To take advantage of entry into the U.S. without a visa, VWP entrants must be coming for less than 90 days for tourism or business. Entrants from VWP countries for other purposes still require a visa.

<sup>7</sup> See Appendix 2.

<sup>8</sup> For a full discussion of the benefits of the visa waiver program, see the GAO report mentioned in the Introduction.

---

According to DHS statistics in fiscal year (FY) 2002, 15.1 million VWP travelers accounted for 3% of U.S. border crossings. By contrast, travelers with visas accounted for 19.3 million crossings, or 5% of the total. Crossings by U.S. citizens - 161.1 million and legal permanent residents - 79.6 million - were 55% of the total, while visa-exempt Canadians -52.2 million- and Mexicans with border crossing cards -104.1 million - comprised 37%. The same data shows that 13 million VWP visitors in FY 2002 arrived by air -86% - while 1.8 million -12% - crossed at land ports and fewer than one-half million -2% - came into sea ports.

While a key aim of the VWP is to facilitate travel to the United States, another essential feature of the program is to reduce the need to process, adjudicate, and issue large numbers of visas, provided that participating countries meet criteria set in U.S. statutes, including reciprocal treatment for U.S. nationals visiting VWP countries. Accomplishment of this visa reduction goal is reflected in figures that show a significant drop - in many cases from two-thirds up to 90% - in nonimmigrant visa issuances to nationals of VWP countries, measured two years before and after entry into the program. For example, in 1987, 1.5 million Japanese received U.S. visas; in 1991, two years after Japan entered the VWP, the number decreased to 130,000. In 1988, British nationals received 950,000 visas; in 1990, the number was less than 350,000.<sup>9</sup>

### **The VWP and Terrorists**

In the changed security environment after the September 11, 2001 attacks against the United States, concerns have been raised that terrorists may take advantage of the VWP to enter the United States or to attack U.S. targets. Among several recent cases we reviewed from public information records are the following:

Habib Zacarias Moussaoui, a French citizen of Moroccan descent, used his French passport without a U.S. visa on February 23, 2001, to fly from London to Chicago, and on to Oklahoma City. There he began flight training at an aviation school in which he had enrolled from abroad. On August 16, 2001, INS arrested Moussaoui because he remained in the United States well beyond the 90 days allowed for VWP entrants and in violation of the requirement that VWP travelers enter for business or tourism. On the basis of intelligence and law enforcement information, he was indicted on December 11, 2001, for engaging in the same preparations as the co-conspirators who carried out the September 11<sup>th</sup> attacks. Moussaoui's trial is in progress.

---

<sup>9</sup> For statistics on all VWP countries, see Appendix 3.



---

Richard Reid, on December 22, 2001, used a British passport newly issued to him in Amsterdam and, without a U.S. visa, boarded American Airlines flight 63 bound from Paris to Miami. Reid's attempt to light explosives hidden in his shoes was foiled by alert passengers and crew. Reid eventually pleaded guilty to multiple federal charges and is serving a life sentence plus 110 years. He was also fined \$2 million.

Ahmed Ajaj fraudulently presented a Swedish passport, on September 1, 1992, with his substituted photo, without a U.S. visa, for INS inspection when he arrived at JFK International Airport on a Pakistani International Airways flight from Peshawar. At secondary inspection, Ajaj's luggage was searched, revealing six bomb-making manuals, notes he had taken during explosives courses, videotapes calling for terrorism against Americans, multiple fake passports and identification documents, and a "cheat sheet" on how to lie to U.S. immigration inspectors. Ajaj was arrested for passport fraud and attempted illegal entry and was serving a six-month sentence when terrorists attacked the World Trade Center (WTC) on February 26, 1993. During his imprisonment, Ajaj had over 20 Arabic-language phone conversations with Ramzi Yousef and other WTC conspirators – undetected at the time. He was released three days after the WTC was bombed. The key figure in that conspiracy, Ramzi Yousef, had entered the United States via the same Pakistan International Airways flight as Ajaj, and they sat together on the first leg of the flight, but took separate seats on the flight inbound to the United States. Yousef had boarded in Peshawar with a fraudulent British passport, presumably with no U.S. visa, and when he arrived at JFK, presented an Iraqi passport in his own name, with no visa. Yousef was sent to secondary inspections where he requested political asylum; he was released on his own recognizance and went on to finish organizing the WTC bombing. After the WTC attack was unraveled, Ajaj's connection with Yousef and other conspirators was discovered. Ajaj was re-arrested, tried, and convicted of conspiracy and other charges, and was sentenced to 240 years in prison and a \$500,000 fine.

According to information from TIPOFF, a terrorist-screening database developed at the Department of State in 1987,<sup>10</sup> between June 1991 and February 2004, more than two hundred VWP nationals were denied entry into the United States following confirmed matches between these individuals and TIPOFF records. Of these, 157 were attempting to enter the United States under the VWP, including:

- A British mercenary who twice was arrested while attempting to enter the United States, the first time in 1991, based on information linking him

---

<sup>10</sup> TIPOFF operations were transferred to the Terrorist Threat Integration Center and the Terrorist Screening Center in 2003.

---

to massacres in Colombia, and then again in 2003, when he was trying to buy a U.S. fighter plane in order to kill renowned drug kingpin, Pablo Escobar.

- A French-Bolivian dual national, who was implicated in a 1990 bombing of the residence of U.S. Marines assigned in La Paz, was apprehended in Miami in 1994 based on TIPOFF records.
- An Irish national applying for admission under the VWP on November 13, 2003, was identified by TIPOFF as a murderer, hijacker, and member of the Provisional Irish Republican Army.
- A Swedish national applied for admission under the VWP on February 3, 2004, at the Rainbow Bridge POE (Buffalo, NY). He possessed a Swedish identification card bearing his photograph and the name of a member of the Mujahedeen-e-Khalq, designated by the Department of State as a terrorist organization.

### **Naturalization Laws and Derived Citizenship**

Some VWP governments, such as Belgium, Sweden, and Denmark, have liberal naturalization laws whereby a third country national can obtain citizenship and a VWP passport after as little as three years' residence. We were told that sometimes inspectors have difficulty determining the admissibility of naturalized VWP nationals because they have reservations with the law enforcement or security history of applicants who have lived in a VWP country for only a few years. Inspectors have little or no opportunity to conduct additional background checks before making a determination that the applicants are eligible to enter the United States. In the words of one inspector: "Our concern is that bad guys can wash their backgrounds clean in only three years."

A second issue involves derivative nationality. In a derivative nationality case, a citizen of one country is able to claim citizenship of a second country – in which the person may never have set foot – because the parents or grandparents are citizens of the second country. Irish nationality, for example, is available to almost anyone with one Irish grandparent. Italian law is even more generous in this respect.



---

## VWP Management

All of the officials we spoke to told us that the VWP is not properly organized or managed. When INS disbanded, the VWP program manager was reassigned to other responsibilities, and several officials filled in on an interim basis or shared responsibility for the VWP requirements. We were told that since the establishment of DHS responsibility for the VWP is unclear. One CBP official described the VWP as being “on autopilot, in an orphan status, with no designated manager or overseer.” This official said the biggest challenge for DHS is to make management decisions so that a cadre of officers from CBP and ICE can be trained to manage the VWP and work with appropriate intelligence components, as well as the Department of State, to get the VWP functioning properly again.

Another CBP official said that DHS must decide how it is going to manage its VWP responsibilities and operations. Then it must select the right manager to address inspections and enforcement issues, conduct inter-agency coordination, and monitor diplomatic and international aspects of the program.

Department of State officials told us that “DHS needs to identify who will be responsible for the VWP program” so that work can proceed on coordinated DHS-Department of State reports, such as the biennial country reviews.<sup>11</sup> Some Department of State officials were told that responsibility for VWP was shifting, or had been shifted to CBP, but that ICE might still be interested in managing the program. Another official was told by a senior DHS manager that the Office of the Assistant Secretary for Policy and Planning was responsible for VWP, but this seems unlikely because that office does not normally exercise operational duties.

POE inspectors and intelligence analysts told us that lines of communication, since the reorganization, regarding the VWP were unclear. For example, intelligence analysts at one airport Passenger Analysis Unit said they no longer knew where to send their VWP-related information and that the guidance they receive from headquarters was random.

### **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

1. Assign responsibility for policy direction of the VWP to a specific office, designate a VWP program manager with clearly defined responsibilities,

---

<sup>11</sup> See discussion of country reviews below.

---

and designate subordinate officials in other DHS components upon which the VWP depends for its coordinated functions.

## VWP Overstay Reporting

We were unable to confirm that DHS submitted required VWP overstay reports. The Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996<sup>12</sup>, requires annual reporting on the number of VWP visitors “for whom no matching departure record has been obtained...with an accounting by the alien’s country of nationality and date of arrival in the U.S.” Without these reports, the government cannot accurately evaluate the potential risks to U.S. security posed by a country’s continued participation in the VWP.

We asked several officials whether any such reports had been submitted, but did not receive clear responses. One official suggested that we ask the congressional liaison office of the former INS, an office that no longer exists. A former INS official said that reports were not submitted and that INS did not have adequate information or records to complete the reports.

The database used to keep records for such information is the Nonimmigrant Information System, a paper-based entry and exit tracking system for nonimmigrant visitors to the United States. It was first deployed in 1983 and remains largely unchanged since then. The system contains a large amount of information accessible to several federal agencies, including entry and exit data. However, one problem for years has been incomplete collection of departure information because the United States lacks a formal exit or departure control system, as exists in most countries. VWP travelers often lost the portion of the Form I-94W that was inserted into their passport when they arrived or failed to turn it in on departure. Moreover, the Form I-94W records were not always properly transmitted, processed, or recorded.

The Visa Waiver Permanent Program Act (VWPPA) of 2000<sup>13</sup> also requires annual reporting, by country, of percentages of VWP arrivals for which no record of departure exists. Data for this reporting requirement was supposed to be collected by a fully automated entry and exit control system to be developed and implemented by October 1, 2001. This system has not been developed as planned. We were unable to confirm that any reports were submitted according to

---

<sup>12</sup> Section 110(b)(2)(C).

<sup>13</sup> Section 205 (a)(1)(C)(i).

---

this requirement. Although we questioned several DHS officials, we were unable to identify which DHS office was responsible for submitting the reports.

A regulation was published in early October 2002 requiring transportation carriers to submit VWP travelers' arrival and departure records electronically. Since October 1, 2002, according to a DHS fact sheet, passenger arrival and departure information on people entering and leaving the United States under the VWP has been electronically collected from airlines and cruise lines through the Advance Passenger Information System (APIS). An official at the US-VISIT Office confirmed that since October 1, 2002, the system for electronic collection of arrival and departure data on VWP travelers was in operation at all required ports of entry. However, the VWP traveler information was available only at seven POEs. We were told that because of technical reasons "only seven of them were fully operable and had the 'class of admission' screen activated." He added that the carriers were providing arrival and departure information at that time, and so "we [DHS] had it." Except for the seven POEs, BTS could not distinguish between VWP travelers and visa travelers. In November 2003, we were told that the system has been further developed, but it was still not fully operational.

Officials at CBP who are responsible for collecting APIS data explained that the series of laws and regulations regarding provision of arrival and departure data emerged in stages. Some legislation refers expressly to VWP travelers while other provisions use more general terms. BTS expects that early in 2004 a new and final regulation will be published which implements recent laws by requiring provision of both arrival and departure data, with penalties, for all foreign travelers. Currently, there are penalties for non-provision of arrival data, but not for non-provision of departure data. Many carriers, however, are providing the departure data anyway. This latter point was confirmed to us in site visits to five ports of entry, where we were also told that enforcement of penalties had persuaded carriers to provide arrival data as required and departure.

### **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

2. Develop a plan to ensure the accurate and timely submission of required VWP annual reports.

---

## VWP Country Reviews

BTS has not conducted required VWP country reviews and has not developed plans to conduct them in the future. As part of strengthened VWP reporting requirements, the VWPPA required the Attorney General, in consultation with the Secretary of State, periodically, but not less than once every five years, to evaluate “the effect of each country’s continued designation on the law enforcement and security interests of the United States...and to determine, based upon the evaluation, whether the designation should be continued or terminated...” The VWPPA required that evaluation reports were to be submitted to appropriate Congressional committees. The requirement for review of each VWP country at least once every five years was changed to every two years.<sup>14</sup>

DHS officials told us that in 2000, the DOJ’s INS and the Department of State’s Bureau of Consular Affairs began to negotiate an “Interagency Protocol for Implementation of the Visa Waiver Program.” The protocol included provisions regarding the designation of new countries, periodic review of continuing designation, emergency termination, and several other provisions. By May 2001, work on the draft protocol had solidified and planning began to form inter-agency teams to visit VWP countries to assess their continuing designation in the program. Before planning was concluded and before the protocol was finalized for submission to department principals for approval, the September 11<sup>th</sup> attacks occurred, resulting in shifting priorities, attention, and resources. The protocol was never formally approved.

In November 2001, however, six inter-agency teams from INS, U.S. Customs, and the Department of State made assessment review visits to Slovenia, Belgium, Italy, Portugal, Argentina, and Uruguay. The purpose of these reviews, pursuant to the VWPPA, was to make in-depth assessments of relevant conditions and practices in VWP countries from the perspective of U.S. law enforcement and national security interests.

Following the teams’ draft reports, the ensuing review process was difficult and protracted. There were sharp internal differences between the INS Office of Inspections and other INS elements, as well as with the Departments of Justice and State, including differences over facts, misunderstandings over contexts, tendentious allegations, and judgments that standards had been unevenly and

---

<sup>14</sup> Section 307(a)(2) of EBSVERA, 2002.

---

inconsistently applied from one country to another. The review process resulted in decisions by the Attorney General to:

- Terminate the designation of Argentina;
- Continue designation of Italy, Slovenia, and Portugal;
- Terminate the designation of Uruguay; and
- Allow Belgium to continue participating in the VWP on a provisional basis for one year, starting from May 15, 2003, with another evaluation to be conducted at that time to determine whether Belgium's continued participation in the VWP is in the law enforcement and security interests of the United States.

When we inquired in November 2003 whether additional VWP reviews had been conducted or were planned, CBP officials told us that there are no plans to conduct any future country reviews. When we asked in particular about Belgium, whose one year provisional participation in the VWP is due to lapse May 14, 2004, CBP officials responded that no plans yet have been made to conduct the follow-up evaluation as stipulated in the Attorney General's March 2003 announcement.<sup>15</sup> Department of State officials told us that they have urged DHS to conduct the VWP reviews, but that DHS has not yet decided to do so.

CBP officials said that the first country reviews had been conducted under the leadership of the INS Office of Inspections. They told us that DHS must create an inter-agency structure similar to the earlier one and the CBP Office for Field Operations is examining this requirement. DHS must also develop standard country review protocols for future country reviews. We were told the country review protocols would most likely resemble the draft protocol.

CBP officials also told us that the new requirement to review VWP countries every two years greatly increased the demands for personnel, resources, and funds to conduct the reviews. However, additional funding to support this requirement was not provided. When asked whether future VWP reviews might be included on the agenda for 2004, CBP officials said this might be possible by the end of 2004, but it would require additional work, resources, and funds.

---

<sup>15</sup> For the Attorney General's statement, see the Federal Register, March 7, 2003, Volume 68, Number 45. It is not clear whether Belgium's provisional participation in the VWP would be extended beyond one year if the follow-up evaluation is not conducted on a timely basis.

---

## **Recommendations**

We recommend that the Under Secretary for Border and Transportation Security:

3. Formally assign responsibility for conducting the required country reviews and develop formal protocols for conducting the reviews.
4. Determine what funds and resources will be necessary to conduct the mandated country reviews.
5. Conduct the review of Belgium as a designated VWP participant to avoid any lapse when its one year provisional status ends on May 14, 2004.

## **Lost and Stolen Passports**

BTS does not have a process to check lost and stolen passport (LASP) information with entry and exit information to determine the scope of fraudulent use of VWP passports. Further, BTS does not collect and analyze data from the POEs regarding the fraudulent use of VWP passports. During the past 15 years, several hundred million VWP visitors have entered the United States and at the same time, many thousands of passports from VWP countries have been lost or stolen.<sup>16</sup> BTS has little information on how many of these passports have been fraudulently used to enter the United States, how many may still be in circulation, how many have and have not been entered into U.S. lookout databases,<sup>17</sup> or who may have used them.<sup>18</sup>

We asked an inspector with extensive experience in passport fraud and travel patterns whether it is possible to check all of the LASP data provided by VWP governments against U.S. databases with entry and exit information, in order to determine the number of times lost or stolen VWP passports have been used to

---

<sup>16</sup> All governments, including VWP participants, face LASP problems. Some VWP governments have bigger problems than others. Among those cited repeatedly to us by port inspectors as having serious problems were Italy, France, Belgium (reported to be formerly a very bad problem, but considerably improved since May 2003), Slovenia (formerly a serious problem, improved since August 2002), and Portugal (a more recent problem). Port inspectors also cited significant LASP problems in the United Kingdom, Denmark, Spain, and Japan (counterfeits).

<sup>17</sup> Section 308 of the Enhanced Border Security and Visa Entry Act of 2002 stipulated that “to the extent practicable,” the Attorney General, in consultation with the Secretary of State, shall establish a system of procedures for tracking stolen passports.

<sup>18</sup> We were provided with a limited amount of information about stolen VWP blank passports subsequently filled in with fraudulent data and used for repeated entries. The OIG will pursue this matter separately.

---

enter the United States. His response was affirmative, and he estimated that it might take three people working about six months to accomplish this task.

Virtually all those familiar with VWP operations told us that LASP is the greatest security problem associated with the VWP. Officials from the law enforcement community, who deal with alien visitors and passports on a daily basis, see the potential for misuse of VWP passports as a security risk, especially since September 11, 2001. They report frequent examples of such misuse, several times a week or more at major international airports. Alien smuggling gangs routinely use fraudulent VWP passports to bring illegal aliens and their escorts to the United States. When we requested data on such misuse of VWP passports at U.S. POEs, a CBP official told us that such data is not collected by country because there has never been a requirement to do so, and in the absence of a requirement, funding was not provided.

FDL officials told us that criminals consider a VWP passport a very valuable commodity. Every time a new country entered the VWP, its passports became targets for counterfeiters, petty crooks who attempt photo substitutions, and organized criminals who steal blank passports, as well as forgers who use modern technology to create false identities in blank passports and criminal rings who manufacture phony identity documents in order to obtain VWP passports. Further, FDL officials said that every time a new country was added to the VWP, the U.S. government effectively increased the number of countries whose passports became fraud threats. FDL stressed that the security of document manufacturing and the issuing process for VWP passports is critical. Therefore, it is essential to review VWP government document manufacturing and issuing practices. The required biennial country reviews are supposed to address these issues. However, BTS has not planned any future country reviews.

### **Recommendations**

We recommend that the Under Secretary for Border and Transportation Security:

6. Develop a procedure to check all LASP data provided by VWP governments to the U.S. government against entry and exit data to assess the magnitude of vulnerability from the fraudulent use of lost and stolen VWP passports and, if possible, to identify and take enforcement measures against travelers who remain in the U.S. after entering fraudulently with such documents.



- 
7. Develop procedures to collect and analyze information collected at POEs regarding any fraudulent use of VWP passports.
  8. Include as part of BTS' country review protocols, the provision to review the security of VWP document manufacturing and issuing practices.

## Reporting LASP Information

FDL and others at DHS told us that there continue to be problems with how the United States obtains LASP information from VWP governments. Obtaining this information is essential in order to build an accurate database against which POE inspectors can check the documents of applicants for entry into the United States.

A CBP official with 13 years experience told us that LASP information for the U.S. database is channeled from foreign authorities primarily through the Department of State. INTERPOL provides LASP data through faxes, while Canadian authorities provide some information directly to the U.S. government. Some government ministries, we were told, contact consular officials at U.S. embassies and give them LASP data; others pass it to the regional security officer at U.S. embassies or to a legal attaché. In some cases, FDL receives information directly from foreign officials. Also, LASP data can be passed to DHS components abroad or in the United States from diplomatic or law enforcement personnel representing VWP governments.

During our visits to VWP countries, we also heard varying accounts of how designated VWP governments provide LASP information to the United States, reflecting a lack of uniformity, inconsistency and differences in practice, and in the case of France, the absence of a bilateral agreement to serve as a formal framework for providing such information.<sup>19</sup>

The director of Passport Services at the Department of State told us that all its LASP data is entered into the Consular Lookout and Support System (CLASS), and from CLASS into Treasury Enforcement Communications System (TECS) and then is available directly to POE inspectors. He said the flow of LASP information from VWP governments currently is "pretty good," and has improved

---

<sup>19</sup> When we asked a group of French passport officials how their government provides LASP data to the United States, some responded that it was provided to U.S. law enforcement contacts through a French police officer at their embassy in Washington. Others were uncertain, and some i□ States. One official said that France provides LASP data to Interpol and to European governments, and through informal channels to the United States.



---

recently. On August 28, 2003, the Department of State sent instructions to all embassies and consulates describing the collection, reporting, and data entry requirements of LASP data. When reported from diplomatic and consular posts, this information is shared simultaneously with DHS through the “Lookout Unit” at CBP’s National Targeting Center.

### **Recommendation**

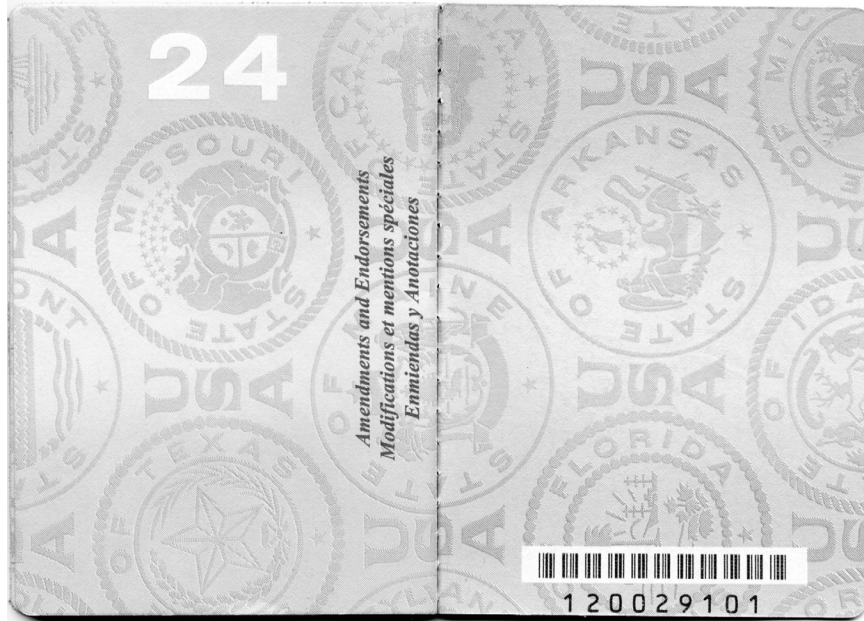
We recommend that the Under Secretary for Border and Transportation Security:

9. In coordination with the Department of State, develop standard operating procedures for the routine and proactive collection of LASP information from host governments for its dissemination to United States agencies.

## **Detection of Stolen VWP Passports**

In March 1999 and December 2001, the DOJ OIG reviewed the VWP and reported a number of key problems regarding LASP issues. One recommendation, made in the first report and reiterated in the second, was that POE inspectors be required to enter the passport number of each VWP applicant, especially of passports that are not machine-readable, to be checked against the lookout system. INS issued such a policy and re-issued it after the second DOJ OIG report. However, we were unable to confirm that any monitoring of compliance with this policy was ever performed.

We encountered another problem relating to LASP information. In most countries, when passports are first manufactured, but before they are assigned to an individual and “personalized” with the intended bearer’s photo and biographic data, they contain a serial number, usually printed inside the rear cover. This is called the “book number” or the “inventory control number” (ICN). In many countries, including the United States, another number is assigned during the personalization process and printed on the biographical page as the “passport number.” Besides being clearly printed on the biographical page as the passport number, this number is coded into the machine-readable strip of a machine-readable passport (MRP). This numbering procedure is referred to as a “two-number system.”



*Inside rear cover of a U.S. Passport, with the inventory control number (book number) and bar-code, as fabricated at U.S. Government Printing Office.*



*Personalized, a different “passport number” appears both in the upper right corner, and also in an OCR font in the machine readable zone.*

---

Foreign governments report stolen blocks of blank passports, which were never issued nor assigned passport numbers, to the U.S. government using the ICNs. The ICNs are entered *en bloc* into U.S. lookout systems. Several years ago, FDL officials reported that they urged that ICNs be entered into the lookout systems individually, not in one batch listing. This would provide the POE inspector with a “one-to-one” hit when the passport was presented. This change in procedure was not effected because of funding delays and the agency re-organization.<sup>20</sup>

The key problem with two number passports is that when *male fide* VWP applicants present stolen passports for inspection they will contain false identity information - including a false passport number. When the inspector enters the false passport number into the lookout system, or enters it by swiping the machine-readable strip, no “hit” or match will occur. This is because the lookout system searched for the passport number, and not the ICN that was entered into the system. The stolen passport will be detected only if the inspector manually enters the ICN and queries the lookout system.

The ICN problem is further complicated by the lack of standardization in numbering systems, including VWP participants and the United States. It is difficult to keep track of which government uses which numbering system and which anti-counterfeit security system, as changes occur in technology and security measures are tightened. Keeping track of these protocols is a task that an expertly trained and experienced inspector may be able to do, but we were told that the task is often very challenging for newer inspectors. For example, one POE inspector told us that the new Belgian passports incorporate the ICN within the machine-readable zone of the document and thought some other new VWP passports do as well; but, he was not sure which ones. FDL prepared a useful summary guide to VWP passports for inspections purposes. It was issued in 2001 and now is being updated.

Government officials in Belgium, France, and Britain told us that each uses the “one number system” recommended by the International Civil Aviation Organization (ICAO), so the ICN will become the passport number when it is issued. In Belgium, the ICN is preceded by two variable alphabetic letters, which are essential in identifying individual passports. Belgian authorities told us that these key alphabetic letters have been or are sometimes dropped by U.S.

---

<sup>20</sup> According to the FDL, the lack of oversight of the lookout system.

---

inspectors when entering stolen Belgian passport numbers into U.S. lookout system. This results in no “hits” or matches.

Brunei and Singapore use the two-number system and the bearer’s passport number is the same as their National Identity Card number. As a result, every passport a particular citizen ever carries will have the one passport number. When a passport is lost or stolen, the citizen’s new passport will have the same number as the one reported lost. Singapore authorities told us that they believe this permanent linkage between citizens and their passport numbers reduces fraud.

Officials of the Passport Services Office at the Department of State told us that passport standardization issues are addressed through ICAO, and ICAO has already recommended that governments use a “one number” system for passports. This means that the ICN would be the same number used after the passport is issued containing personal identity information, and it would also be in the machine-readable zone; this, taken together with the pending development of biometric information included in passports, would defeat all but the most skillful attempts to forge stolen blank passports.

Additionally, the Department of State’s Passport Services Office official told us that when the new biometric U.S. passport is introduced in October 2004, it will adopt the one number system for the first time. The United States also will support efforts within ICAO to change its one number recommendation to a uniform numbering standard that is required of participating governments. The new ICAO standard will be a positive development when it occurs, but it will take years for “one number” passports to replace the existing multiplicity of passport numbering systems in international use. The intervening years will see continuing vulnerability to forgery and fraudulent use of stolen blank passports, especially from VWP countries.

### **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

10. Require that inspectors query the lookout systems using both the passport number and the ICN for VWP passports from countries that use the two number system.

---

## Stolen Passports are Returned to Travelers

POE inspectors cited another LASP problem that occurs with certain fraudulent VWP travelers. If the inspector identifies a lost or stolen passport while interviewing an applicant for entry – for example one that has been photo-substituted or otherwise altered – the applicant will be denied entry, but the fraudulent document must be given back to the traveler. The traveler then might return to the foreign port of departure with these fraudulent documents in hand. Inspectors told us that if they were allowed to keep these false documents it would have the benefit of removing them from circulation, as well as serve as training exemplars for new inspectors, who gain most of their knowledge and experience on the job. We were told that there may be internationally accepted provisions for providing “travel letters” to permit fraudulent travelers to be returned to foreign destinations without their fraudulent documents, but cases were cited in which such letters were refused by foreign authorities and the fraudulent travelers were sent back to the United States. The result is that in most cases, inspectors return fraudulent documents to applicants after denying them admission in order to facilitate their reception in the country to which they are being returned.

### **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

11. Review the basis for the practice of returning fraudulent passports to applicants denied admission, and if feasible, issue policy guidance that would allow fraudulent passports to be seized by port inspectors or other appropriate U.S. authorities.

## US-VISIT and VWP

Currently, VWP travelers are excluded from processing through the US-VISIT system. On January 5, 2004, DHS announced the launching of US-VISIT at 115 airports as well as cruise ship terminals at 14 seaports. US-VISIT established new entry procedures for most foreign travelers with non-immigrant visas, using biometric technologies – fingerprint scans and digital photographs – to verify travelers’ identities. US-VISIT procedures facilitate more thorough screening against criminal and terrorist databases and provide a “one-to-one” check linking the visitor with a specific travel document. When announcing US-VISIT, DHS said that visitors who seek to enter the United States under the VWP will not



---

be affected by the US-VISIT program “at this time.” Thus, VWP visitors are not subject to the finger-scan and digital photograph procedures of US-VISIT. Accordingly, screening of VWP visitors against criminal and terrorist databases is less thorough than screening for travelers with visas. In addition, POE inspectors cannot make a “one-to-one” check linking a VWP traveler with a specific passport or travel document, increasing the potential risk of identity or document fraud by *male fide* travelers who abuse the VWP.

Officials from the US-VISIT Office, CBP, and BTS provided us different perspectives regarding the decision to exclude VWP travelers. CBP and US-VISIT officials told us that VWP travelers would be included in US-VISIT procedures at an indeterminate time in the future. Several officials said that the decision not to include VWP travelers at the outset rested upon practical considerations and the need to implement the complex, nation-wide new national US-VISIT procedures in stages. We were told that earlier efforts to set up an automated entry-exit system had shown that it was advisable to proceed in steps, because as the infrastructure is expanded, the software is adapted and experience is acquired. While we were told that there are logistical arguments supporting deferment of VWP entry into US-VISIT, we did not find a firm commitment to apply US-VISIT procedures to VWP travelers eventually. According to one BTS policy official, no such decision has been made.

POE inspectors were generally unsympathetic to the justification for excluding VWP travelers from US-VISIT. Several inspectors commented that VWP travelers should be the first ones to be finger-scanned and photographed because travelers with visas have already gone through an extensive screening process that includes being photographed and finger-scanned at the embassy or consulate before arriving in the United States. They said that while VWP travelers in general are considered “low risk” relative to those from countries not in VWP, there are sufficient problems with VWP travelers to constitute an added security risk. From an enforcement perspective, it makes sense to take every step available to reduce such risks, they said.

The following description highlights the concerns of the POE inspectors. While the name-based database checks conducted at POEs are the same for all travelers - visa or VWP - the visa travelers receive an additional check provided by US-VISIT. Visa travelers, even after undergoing previous background checks, have their fingerprints taken and checked at the POE. This check, at the time of visa application, constitutes a security advantage because it runs the traveler against fingerprint or biometric databases that cannot be done with names alone. If a

---

VWP traveler appearing at POE falsely claiming to be John Smith presents what appear to be valid documents, the inspector will run the name “John Smith” in the database. If there is no record for “John Smith,” there will be no match against any watch list or warrants list. However, if John Smith is traveling on a visa, he will also have his fingerprints taken. Since January 2004, there have been dozens of examples of persons claiming to be “John Smiths” but after the fingerprint checks are run, they turn out to be wanted felons or suspected terrorists known by another name. If “John Smith,” however, enters on the VWP, he will not be fingerprinted, the derogatory information under the false name will not be discovered, and he will not be apprehended or removed. This is the argument for running all visitors through US-VISIT.

However, not everyone with law enforcement experience shared this view. Three DHS officials with extensive inspections background expressed support for the need to implement US-VISIT in stages and to delay inclusion of VWP applicants under its procedures, because of the positive benefits of the VWP and lack of evidence over the years that it poses a serious security risk.

Conversely, several experts in passenger analysis and fraud prevention predicted that soon after implementation of US-VISIT procedures, there will be increased efforts by terrorists and counterfeiters to obtain or produce VWP travel documents and to use them for travel to the United States and elsewhere. *Male fide* applicants will seek to avoid providing fingerprints and digital photographs, and the demand for VWP documents and their fraudulent use will increase. We were told by several POE inspectors and intelligence analysts that certain VWP passports, e.g., Britain, France, Spain, Australia, and Denmark, already are preferred documents for terrorist groups. The non-inclusion of VWP applicants under US-VISIT procedures can be expected to push these groups toward increased use of VWP passports.

One DHS official suggested that for security reasons US-VISIT procedures should be applied to all applicants unless they present documents that incorporate biometric identifiers. Widespread use of VWP passports with biometric identifiers, however, lies years in the future. Another U.S. intelligence official told us that he does not expect terrorist groups to make increased use of counterfeit VWP passports, but to target the document issuing process itself, by creating or forging fictitious identities in order to obtain genuine VWP passports with all the latest security features in them.

---

The majority of opinions we heard favored the inclusion of VWP travelers in the US-VISIT procedures. While some officials defended the decision to defer this step, their view was that eventually it should happen. The ambiguity as to whether VWP travelers will in the future be subjected to US-VISIT procedures seems avoidable and suggests a gap in long-range investment and business planning that should be addressed.

### **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

12. Include VWP travelers under US-VISIT procedures as soon as the program is capable of handling them.<sup>21</sup>

## **Biometric Passport Deadline**

Department of State officials told us that most of the 27 designated VWP countries will not meet the deadline of October 26, 2004, for complying with EBSVERA, which requires a country to issue machine readable, tamper resistant passports with biometric and document identifiers that comply with ICAO standards.<sup>22</sup> EBSVERA required<sup>23</sup> that any alien applying for admission under the VWP on or after October 26, 2004, present a passport that meets those requirements, unless the alien's passport was issued prior to that date. The legislation does not provide waiver authority regarding those provisions.

The Department of State now is facing what one official calls "a train wreck" on October 27, 2004, the date when the VWP would become unavailable as a travel option for large numbers of travelers without biometric ICAO compliant passports. Department of State officials told us this would necessitate the processing and adjudication of an estimated 3 to 5 million additional visa applications, and at least short-term hiring of hundreds of additional consular officers and foreign nationals to do this unbudgeted and unplanned work. Also, the disruption of the VWP may result in significant changes in traveler patterns at U.S. POEs, creating staffing and other resource shortages.

---

<sup>21</sup> On April 2, 2004, after the release of our draft report, DHS issued a press release stating that it will begin enrolling VWP travelers through the US-VISIT program at all airports and seaports by September 30, 2004.

<sup>22</sup> Section 303 (c)(1) of Enhanced Border Security and Visa Entry Reform Act of 2002.

<sup>23</sup> EBSVERA, Section 303(c)(2).



---

## **Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

13. Develop and recommend legislation to provide waiver authority regarding the October 26, 2004, deadline or provide a report on its preparation to meet the changes in BTS' workload.<sup>24</sup>

## **POE Inspector Training**

Lack of training hampers POE inspectors' efforts to detect VWP passport fraud. At Newark International Airport, we had an extended discussion on the benefits of and problems with the VWP with a group of experienced POE inspectors. POE inspectors emphasized their respect for today's visa issuing process at U.S. consulates as well as the visa's security features, contrasting this with the brief POE inspection given a VWP applicant. The group strongly agreed that POE inspectors need more and better training on passport fraud, especially with VWP passports where the applicant will have no prior screening. They noted that the 12-week training course for new inspectors at the Federal Law Enforcement Training Center devotes only one day to passport fraud. New inspectors learn most of their passport fraud detection skills on the job, and in the learning process make mistakes that more seasoned inspectors would avoid.

We were told that FDL provides invaluable information. FDL experts once provided instruction at POEs. One inspector stated that he attended a training program years ago, but did not know if the program still existed. Most training on passport fraud is conducted locally at the POEs. Some POEs have sent small teams of experienced inspectors to provide short instructional courses at other POEs, but these efforts were curtailed because of inadequate funds. A senior FDL official emphasized that "the biggest gap of all in our security system today is in the great need for increased investment in our front-line inspections officers."

Compounding the training issue is the high attrition of POE inspectors. POE inspectors told us that over the past four years attrition rates for POE inspectors at JFK International Airport has ranged between ten and twenty percent annually.<sup>25</sup>

---

<sup>24</sup> The A□ deadline for two years.

<sup>25</sup> A CBP official from the New York City office provided the following attrition figures for JFK for the past four fiscal years: FY 00: 46 out of 453 = 10.2 percent; FY 01: 67 out of 453 = 14.8 percent; FY 02: 96 out of 460 = 20.9 percent; FY 03: 73 out of 471 = 15.5 percent.

---

The attrition problem worsened recently when the Transportation Security Administration announced the expansion of the federal air marshals program. We were told that the turnover rate at Newark International Airport over the past year was the highest ever – more than 50 percent. Many junior inspectors immediately left to become federal air marshals because of better pay, greater career mobility, shorter hours, and better retirement benefits. Because air marshals are designated federal law enforcement personnel, they receive higher pay and can retire much earlier. With the filling of the federal air marshals' ranks, the hemorrhage of inspectors has slowed.

**Recommendation**

We recommend that the Under Secretary for Border and Transportation Security:

14. Develop a training program for inspectors to ensure that they acquire, retain and enhance their abilities to detect fraud at the POEs.

**Countries in the Visa Waiver Program**

<b><u>Country</u></b>	<b><u>Date Added to Visa Waiver Program</u></b>	<b><u>Date Removed From Visa Waiver Program</u></b>
Great Britain and Northern Ireland	07/01/88	
Japan	12/15/88	
France	07/01/89	
Switzerland	07/01/89	
Germany	07/15/89	
Italy	07/15/89	
Netherlands	07/29/89	
Sweden	07/29/89	
Andorra	10/01/91	
Austria	10/01/91	
Belgium	10/01/91	
Denmark	10/01/91	
Finland	10/01/91	
Iceland	10/01/91	
Liechtenstein	10/01/91	
Luxembourg	10/01/91	
Monaco	10/01/91	
New Zealand	10/01/91	
Norway	10/01/91	
San Marino	10/01/91	
Spain	10/01/91	
Brunei	07/29/93	
Ireland	04/01/95	
Argentina	07/08/96	02/21/02
Australia	07/29/96	
Slovenia	10/20/97	
Portugal	08/09/99	
Singapore	08/09/99	
Uruguay	08/09/99	04/15/03

## Appendix 2

### Nonimmigrant Admissions for Visa Waiver Program Countries, 1998 - 2003

<b>Fiscal Years 1998-2003</b>						
	1998	1999	2000	2001	2002	2003 <sup>1</sup>
<b>Total VWP</b>	<b>15,792,630</b>	<b>16,518,759</b>	<b>17,697,919</b>	<b>16,582,603</b>	<b>13,230,001</b>	<b>13,520,950</b>
Andorra	588	686	723	573	386	478
Argentina <sup>2</sup>	300,607	353,240	410,915	443,047	89,695	X
Australia	418,615	451,158	519,176	478,688	445,389	483,423
Austria	179,559	195,835	190,194	153,008	107,636	114,976
Belgium	206,671	223,961	234,136	197,660	166,286	155,391
Brunei	667	666	615	568	303	323
Denmark	131,801	142,185	151,417	143,559	124,819	141,654
Finland	78,941	88,908	99,266	86,796	71,342	73,399
France	1,050,173	1,141,334	1,193,256	1,075,677	932,853	918,691
Germany	1,837,930	1,972,189	1,893,534	1,525,268	1,208,127	1,251,703
Iceland	19,165	24,013	24,462	21,648	17,733	19,773
Ireland	230,244	292,625	338,793	345,623	297,497	305,205
Italy	686,572	723,149	737,641	670,751	515,135	575,077
Japan	4,998,309	4,740,097	4,942,818	4,752,948	3,348,087	3,300,513
Liechtenstein	1,343	1,394	1,392	1,365	996	993
Luxembourg	12,270	12,817	11,141	8,243	6,001	6,433
Monaco	559	671	677	586	377	432
Netherlands	538,083	579,923	623,088	538,967	486,672	497,337
New Zealand	143,714	151,356	171,403	168,417	187,281	180,494
Norway	128,293	135,110	139,728	134,515	110,713	119,638
Portugal <sup>3</sup>	X	7,118	66,779	72,402	57,251	64,030
San Marino	527	522	531	398	279	300
Singapore <sup>3</sup>	X	5,636	66,521	68,434	49,792	54,521
Slovenia	11,543	14,938	16,119	13,155	6,951	9,658
Spain	325,574	371,577	394,170	369,543	350,045	374,066
Sweden	275,065	300,344	317,515	273,100	198,532	220,256
Switzerland	312,543	313,724	322,935	291,764	228,300	220,679
United Kingdom	3,757,298	4,088,050	4,563,621	4,487,214	3,939,679	4,170,466
Uruguay <sup>3,4</sup>	X	3,802	33,625	40,931	35,705	23,433
Unknown	145,976	181,731	231,728	217,755	246,139	237,608

<sup>1</sup> Preliminary data.

<sup>2</sup> Removed from Program February 2002.

<sup>3</sup> Admitted to Program August 1999.

<sup>4</sup> Removed from Program April 2003.

X Not applicable.

Appendix 3  
 Nonimmigrant Visa Issuances in VWP Countries Before and After VWP Accession

**Nonimmigrant Visa Issuances in VWP Countries Before and After VWP Accession**

Entered Program during FY-1988

Nationality (admitted)	1986	1987	1988	1989	1990
Great Britain and Northern Ireland(7/88)	651,075	784,203	955,739	543,138	347,476

Entered Program during FY-1989

Nationality (admitted)	1987	1988	1989	1990	1991
Japan (12/88)	1,538,725	1,789,598	351,947	141,091	132,696
France (7/89)	382,345	374,353	270,129	97,490	96,630
Switzerland (7/89)	125,138	145,793	125,555	65,659	65,517
Germany, Fed Republic of (7/89)	583,539	702,557	521,345	189,356	182,446
Italy (7/89)	226,762	249,833	196,456	42,197	38,258
Netherlands (7/89)	157,101	186,173	164,261	71,810	59,185
Sweden (7/89)	117,878	144,441	135,253	22,672	32,018

Entered Program during FY-1992

Nationality (admitted)	1990	1991	1992	1993	1994
Andorra (10/91)	128	190	22	29	29
Austria (10/91)	96,411	79,490	8,210	6,906	6,948
Belgium (10/91)	71,744	78,232	11,534	8,007	6,499
Denmark (10/91)	71,245	62,641	15,843	17,124	18,862
Finland (10/91)	73,886	64,006	6,895	6,285	6,324
Iceland (10/91)	7,815	7,763	2,816	3,103	2,834
Liechtenstein (10/91)	517	487	47	72	83
Luxembourg (10/91)	4,180	4,921	701	699	776
Monaco (10/91)	143	147	19	21	17
New Zealand (10/91)	93,237	74,920	19,191	15,544	15,699
Norway (10/91)	62,134	48,907	9,787	9,101	10,033
San Marino (10/91)	214	167	16	8	20
Spain (10/91)	171,874	187,383	40,356	28,692	25,447

## Appendix 3

### Nonimmigrant Visa Issuances in VWP Countries Before and After VWP Accession

---

#### Entered Program during FY-1993

Nationality (admitted)	1991	1992	1993	1994	1995
Brunei (7/93)	555	716	585	341	346

#### Entered Program during FY-1995

Nationality (admitted)	1993	1994	1995	1996	1997
Ireland (4/95)	82,606	92,337	45,932	14,514	14,573

#### Entered Program during FY-1996

Nationality (admitted)	1994	1995	1996	1997	1998
Argentina (7/96)	168,224	152,715	111,684	11,226	12,089
Australia (7/96)	250,542	265,308	268,667	26,973	28,044

#### Entered Program during FY-1998

Nationality (admitted)	1996	1997	1998	1999	2000
Slovenia (10/97)	9,883	10,792	1,609	1,227	1,212

#### Entered Program during FY-1999

Nationality (admitted)	1997	1998	1999	2000	2001
Portugal (8/99)	47,711	45,619	42,872	5,576	4,685
Singapore (8/99)	63,159	50,379	35,423	7,475	7,991
Uruguay (8/99)	23,274	22,314	16,776	2,395	2,486

### **Legislative History**

The Immigration Reform and Control Act of 1986 (IRCA)<sup>1</sup> was designed to help control illegal immigration to the United States and to remove the stigma attached to longtime resident undocumented aliens. It provided for the establishment of a Visa Waiver Pilot Program (VWPP), which waives visa requirements for certain aliens seeking admission to the United States for a period of less than 90 days.

To be eligible for a visa waiver, IRCA stipulates that an alien:

- Applies as a non-immigrant visitor pursuant to 8 USC 1101 for a period not exceeding 90 days;
- Is a national of a country that extends reciprocal privileges to citizens and nationals of the United States, and that country is designated under the VWPP;
- Executes a waiver of review and appeal of an immigration officer's determination as to admissibility, or to contest, other than on the basis of an application for asylum, any action for deportation against the alien;
- Possess a round-trip, nontransferable transportation ticket valid for a period of not less than one year, issued by a carrier which has entered into an agreement to indemnify the United States if the visitor is refused admission or remains in the United States unlawfully after the 90-day period, and the carrier has agreed to submit daily to immigration officers any immigration forms received with respect to visitors provided visa waivers;
- Does not represent a threat to the welfare, health, safety, or security of the United States; and
- Complied with the conditions of any previous admission.

IRCA stipulates conditions before the VWPP could be put into operation, including requirements for the Attorney General to:

- Develop a form (I-94W) for use under the VWPP;<sup>2</sup>

---

<sup>1</sup> P.L. 99-603.

<sup>2</sup> This form became the I-94 W form submitted by VWP applicants when presenting themselves for admission into the United States.

- In cooperation with the Secretary of State, develop and establish an automated data arrival and departure control system to screen and monitor the arrival into and departure from the United States of nonimmigrant visitors who receive a visa waiver; and
- Notify Congress certifying that the required form has been developed, and the required screening and monitoring system is operational and effective.

IRCA authorized the participation of up to eight countries, jointly designated by the Attorney General and the Secretary of State, for the VWPP. Initial qualifications for designated countries included (a) a low nonimmigrant refusal rate (less than 2 percent) for the previous two-year period; and, (b) a low nonimmigrant refusal rate (less than 2.5 percent) for each of the two previous years. Continuing qualification each fiscal year for designated countries required that in the previous fiscal year, fewer than 2 percent of nonimmigrant applicants from that country were excluded from admission, withdrew their applications, or violated the terms of admission. IRCA also included prohibitions against any adjustment of nonimmigrant status or adjustment to immigrant status by visa waiver visitors.

Between July 1, 1988, and July 29, 1989, eight countries were designated jointly by the Attorney General and the Secretary of State to participate under the VWPP: Great Britain and Northern Ireland, Japan, France, Switzerland, Germany, Italy, Netherlands, and Sweden.<sup>3</sup>

The Immigration Act of 1990 (IMMACT), P.L. 101-649, in Section 201, amended the VWPP by removing the eight-country cap and extending the provisions to all countries that met the qualifying provisions in Section 217 of the Act. IMMACT added two new qualifications for countries designated to participate in the VWP: that the government of the country certifies that it is in the process of developing a program to issue machine-readable passports to its citizens; and that the Attorney General determines that the United States enforcement interests would not be compromised by the designation of the country. IMMACT also extended the period for the VWPP until September 30, 1994. On October 1, 1991, thirteen additional countries were designated to participate under the VWPP: Andorra, Austria, Belgium, Denmark, Finland, Iceland, Liechtenstein, Luxembourg, Monaco, New Zealand, Norway, San Marino, and Spain. On July 29, 1993, Brunei was designated to participate under the VWPP.

The Immigration and Nationality Technical Corrections Act of 1994, P.L. 103-416, extended the expiration date of the VWPP until September 30, 1996, and created a new “probationary” category for VWPP participation. Ireland was added as a VWPP country on a probationary basis in 1995, upon publication of an interim regulation in the Federal Register (60 FR 15855). Argentina and Australia were added in 1996.

---

<sup>3</sup> For a chronological listing of designation of VWP countries, see Appendix 1.



The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), P.L. 104-208, amended Section 217 of the Immigration and Nationality Act by extending the VWPP until September 30, 1997. IIRIRA also named the Attorney General as the principal designator of VWPP countries, eliminated probationary VWPP qualification status, and made countries then in such status (Ireland being the only country) permanent participating VWPP countries subject to the same disqualification criteria established for other VWPP countries.

In April 1998, the INA was modified to extend the visa waiver pilot program through April 30, 2000, and to provide for the collection of data with respect to the number of nonimmigrants who remain in the United States after the expiration of the period of stay authorized by the Attorney General. The law also modified statutory language relating to low refusal rates that could extend the VWPP to additional countries previously unable to qualify.<sup>4</sup> Slovenia was added as a VWPP country in 1997; Portugal, Singapore, and Uruguay were added in 1999. Statutory authority for the VWPP expired on April 30, 2000, but the INS Commissioner exercised the Attorney General's parole authority to extend the program temporarily.

The Immigration and Naturalization Service Data Management Improvement Act (DMIA) of 2000, P.L. 106-215, required the Attorney General to implement an integrated entry and exit data system in an electronic format. The system, using available alien arrival and departure data, was to be implemented at airports and seaports not later than December 31, 2003, and at high-traffic land border ports not later than December 31, 2004. DMIA required the Attorney General to submit annual reports following commencement of the integrated entry and exit data system. In addition to numbers of alien arrivals and successful departure matches, the reports are to show "the number of aliens who arrived pursuant to a nonimmigrant visa, *or as a visitor under the visa waiver program* (italics added), ...for whom no matching departure data have been obtained... with an accounting by the alien's country of nationality and date of arrival in the United States."

On October 30, 2000, the Visa Waiver Permanent Program Act (VWPPA), P.L. 106-396, was enacted "to amend the Immigration and Nationality Act to make improvements to, and permanently authorize, the visa waiver pilot program under section 217 of such Act." Besides making this program's authorization permanent, the VWPPA included other provisions designed to strengthen documentary and reporting requirements. Among the VWPPA provisions are:

- By October 1, 2007, all entrants under the VWP must have machine-readable passports;<sup>5</sup>

---

<sup>4</sup> Initial qualifications for newly designated VWP countries as stipulated in IRCA of 1986 were a low nonimmigrant visa (NIV) refusal rate (less than two percent) for the previous two-year period and a low NIV refusal rate (less than 2.5 percent) for each of the previous two years. P.L. 105-173 modified this by adding a definition of low NIV refusal rate as "less than three percent for the previous full fiscal year."

<sup>5</sup>IMMACT in 1990 required a qualifying VWP government to certify that it is in the process of developing a program to issue machine-readable passports to its citizens. IMMACT did not specify a date by which VWP entrants would have to present machine-readable passports. Subsequent to the VWPPA, the USA PATRIOT Act dated October 25, 2001, advanced the deadline for VWP entrants to have

- All VWP applicants must be checked against an automated electronic database containing information about the inadmissibility of aliens;
- The Attorney General, in consultation with the Secretary of State, shall evaluate the effect of each program country's continued designation on the law enforcement and security interests of the United States, not less than once every five years;
- By October 1, 2001, the Attorney General shall develop and implement a fully automated entry and exit control system that will collect a record of arrival and departure for every alien who arrives and departs by sea or air at a port of entry in to the United States and is provided a waiver under the program;<sup>6</sup>
- By October 1, 2002, no waiver may be provided to an alien arriving by sea or air unless the carrier is electronically transmitting passenger data to the automated entry and exit control system; and
- The calculation of visa refusal rates for determining country eligibility shall not include any refusals based on race, sex, or disability.

In the wake of the September 11, 2001, terrorist attacks, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, P.L. 107-56, in the context of providing for strengthened measures for aliens visiting the United States:

- Advanced the deadline for VWP aliens to present machine-readable passports from 2007 to 2003.
- Provided limited waiver authority to the Secretary of State for the period beginning October 1, 2003, and ending September 30, 2007, with respect to nationals of a VWP country, if the Secretary finds that the program country is making progress toward ensuring that machine readable passports are generally available to its nationals; and has taken appropriate measures to protect against misuse of passports the country has issued that are not machine readable.

---

machine-readable

the USA PATRIOT Act to waive this requirement for nationals of 22 of the 27 VWP countries.

<sup>6</sup>The Immigration and Naturalization Service Data Management Improvement Act of 2000 mandated the Attorney General to implement an integrated land

border ports of entry by December 31, 2004; and at all ports of entry by December 31, 2005.

In a broader context, and without specific reference to the VWP, the USA PATRIOT Act also:

- Mandated the Attorney General and the Secretary of State jointly, within two years, to develop and certify a technology standard for the purpose of conducting background checks and confirming identity with respect to persons applying for a U.S. visa or seeking to enter the United States pursuant to a visa.
- Provided that the Secretary of State, in the Secretary's discretion and on the basis of reciprocity, may provide to a foreign government information in the Department of State's computerized visa lookout database and, when necessary and appropriate, other records covered by this section related to information in the database.

The Aviation Transportation Security Act of 2001, P.L. 107-071, did not contain any provisions expressly referring to the VWP. Section 115 of the act established a requirement for air carriers operating flights to the United States to transmit electronically a passenger and crew manifest to the Commissioner of Customs. Such information was already required for VWP travelers under the VWPPA.

The Enhanced Border Security and Visa Entry Reform Act (EBSVERA), P.L. 107-173, established a technology standard for visa waiver participants, which requires that not later than October 26, 2004, the government of each country designated as a VWP participant shall certify, as a condition for designation or continuation of that designation, that it has a program to issue to its nationals machine-readable passports. These new passports are to be tamper-resistant and incorporate biometric and document authentication identifiers that comply with applicable standards established by the International Civil Aviation Organization. Also, it required that on and after October 26, 2004, any alien applying for admission under the VWP shall present a passport that meets these requirements unless the alien's passport was issued prior to that date. No waiver authority was granted regarding the October 26, 2004, deadline for these provisions.<sup>7</sup>

EBSVERA further amended the Immigration and Nationality Act, Section 217 (c)(2), to require that the government of the country certifies that it reports to the United States on a timely basis the theft of blank passports issued by that country. EBSVERA did not specify whether such certification was to be on a recurring basis; and "on a timely basis" was not further defined. Additional provision was made, however, that if the Attorney General<sup>8</sup> and the Secretary of State jointly determine that the (VWP) country is not reporting the theft of blank passports, as required

---

<sup>7</sup> For these provisions, see EBSVERA Section 303 (c) (1) and (2).

<sup>8</sup> Subsequent legislation transferred this authority to the Secretary of Homeland Security.

by EBSVERA, the Attorney General shall terminate the designation of the country as a program country.<sup>9</sup>

Argentina was removed as a VWP participant in 2002. The Department of Justice, in consultation with the Department of State, determined that Argentina's participation in the VWP was inconsistent with the U.S. interest in enforcement of the immigration laws of the United States. This determination was made following an economic crisis in Argentina and an increase in the number of Argentine nationals attempting to use the VWP to live and work illegally in the United States. Uruguay was removed as a VWP participant in 2003. The Attorney General's decision to terminate Uruguay's participation in the VWP was based on the high intercept and overstays rates for Uruguayans.

---

<sup>9</sup> See EBSVERA Section 307 for these provisions.

## **Management Comments**

On March 11, 2004, a copy of our draft report was provided to BTS for comment. We requested that BTS respond to the draft report within 30 days. We would have included BTS' response in this appendix of the final report. As of April 20, 2004, we have not received BTS' comments. We attempted to contact BTS officials several times to ascertain the status of the response but received no replies.

## **OIG Evaluation of Management Comments**

BTS did not submit comments to our draft report and therefore, we consider all recommendations unresolved.

## **OIG Recommendations to the Under Secretary of the Bureau of Transportation and Border Security**

1. Assign responsibility for policy direction of the VWP to a specific office, designate a VWP program manager with clearly defined responsibilities, and designate subordinate officials in other DHS components upon which the VWP depends for its coordinated functions.
2. Develop a plan to ensure that accurate and timely submission of required VWP annual reports.
3. Formally assign responsibility for conducting the required country reviews and develop formal protocols for conducting the reviews.
4. Determine what funds and resources will be necessary to conduct the mandated country reviews.
5. Conduct the review of Belgium as a designated VWP participant to avoid any lapse when its one year provisional status ends on May 14, 2004.
6. Develop a procedure to check all LASP data provided by VWP governments to the U.S. government against entry and exit data to assess the magnitude of vulnerability from the fraudulent use of lost and stolen VWP passports and, if possible, to identify and take enforcement measures against travelers who remain in the U.S. after entering fraudulently with such documents.
7. Develop procedures to collect and analyze information collected at POEs regarding any fraudulent use of VWP passports.
8. Include as part of BTS' country review protocols, the provision to review the security of VWP document manufacturing and issuing practices.
9. In coordination with the Department of State, develop standard operating procedures for the routine and proactive collection of LASP information from host governments for its dissemination to United States agencies.
10. Require that inspectors query the lookout systems using both the passport number and the ICN for VWP passports from countries, which use the two number system.

11. Review the practice of returning fraudulent passports to applicants denied admission, and if feasible, issue policy guidance that would allow fraudulent passports to be seized by port inspectors or other appropriate U.S. authorities.
12. Include VWP travelers under US-VISIT procedures as soon as the program is capable of handling them.
13. Develop and recommend legislation to provide waiver authority regarding the October 26, 2004, deadline or provide a report on its preparation to meet the changes in BTS' workload.
14. Develop a training program for inspectors to ensure that they acquire, retain and enhance their abilities to detect fraud at the POEs.



Douglas Ellice, Senior Inspector  
(202) 254-4181  
Douglas.Ellice@dhs.gov

Kenneth McKune, Senior Inspector  
(202) 254-4220  
Ken.McKune@dhs.gov

**Department of Homeland Security**

Deputy Secretary  
Chief of Staff  
DHS Liaison  
Ambassador Cresencio Arcos, Director, Office of International Affairs  
Robert Bonner, Commissioner, U.S. Customs and Border Protection  
Assistant Secretary Michael Garcia, U.S. Immigration and Customs  
Enforcement

**Department of State**

Ambassador Maura Harty, Assistant Secretary for Consular Affairs  
Robert B. Peterson, Assistant Inspector General for Inspections

**Office of Management and Budget**

Homeland Bureau Chief  
DHS OIG Budget Examiner

**Congress**

Congressional Oversight and Appropriations Committee as Appropriate



### **Additional Information and Copies**

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, or visit the OIG web site at [www.dhs.gov](http://www.dhs.gov).

### **OIG Hotline**

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations, call the OIG Hotline at 1-800-323-8603; write to Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.