

July 2007

# BORDER SECURITY

## Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use



# BORDER SECURITY

## Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use

### Why GAO Did This Study

Travel documents are often used fraudulently in attempts to enter the United States. The integrity of U.S. passports and visas depends on the combination of well-designed security features and solid issuance and inspection processes. GAO was asked to examine (1) the features of U.S. passports and visas and how information on the features is shared; (2) the integrity of the issuance process for these documents; and (3) how these documents are inspected at U.S. ports of entry. We reviewed documents such as studies, alerts, and training materials. We met with officials from the Departments of State, Homeland Security, and Commerce’s National Institute of Standards and Technology, and U.S. Government Printing Office, and with officials at seven passport offices, nine U.S. ports of entry, two U.S. consulates in Mexico, and two Border Crossing Card production facilities.

### What GAO Recommends

GAO recommends that State and DHS better plan for new generations of passports and visas, address potential vulnerabilities in the acceptance process of U.S. passport applications, utilize the electronic features of the new e-passport, better use the biometric feature of BCCs, and provide inspectors with systematic training prior to the issuance of new travel documents. State and DHS agreed with our recommendations.

[www.gao.gov/cgi-bin/getrpt?GAO-07-1006](http://www.gao.gov/cgi-bin/getrpt?GAO-07-1006).

To view the full product, including the scope and methodology, click on the link above. For more information, contact Jess T. Ford at (202) 512-4268 or [fordj@gao.gov](mailto:fordj@gao.gov).

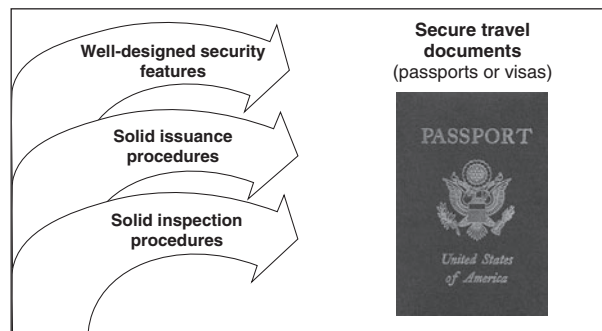
### What GAO Found

The Department of State (State) has developed passports and visas, including border crossing cards (BCC), that are more secure than older versions of these documents; however, older versions have been fraudulently used and remain more vulnerable to fraud during their lifespan. For example, earlier versions valid until 2011, of which there are more than 20 million in circulation, remain vulnerable to fraudulent alteration by such means as photo substitution. Although State has updated or changed the security features of its travel documents, State does not have a structured process to periodically reassess the effectiveness of the security features in its documents against evolving threats and to actively plan for new generations.

State has taken a number of measures to ensure the security and quality of passports and visas, including establishing internal control standards and quality assurance measures, training of acceptance agents, and initiating new visa policies and procedures. However, additional measures are needed in the passport issuance process to minimize the risk of fraud. State lacks a program for oversight of the thousands of passport acceptance facilities that serve an important function in verifying the identity of millions of passport applicants each year.

Officers in primary inspection—the first and most critical opportunity to identify fraudulent travel documents at U.S. ports of entry—are unable to take full advantage of the security features in passports and visas. These officers rely on both their observations of travelers and visual and manual examination of documents to detect fraudulent documents. However, the Department of Homeland Security (DHS) has not yet provided most ports of entry with the technology tools to read the new electronic passports and does not have a process in place for primary inspectors to utilize fingerprints collected for visas, including BCCs, at all land ports of entry. Moreover, DHS has provided little regular training to update its officers on the security features and fraud trends in passports and visas.

#### Key Elements of a Secure Travel Document



Source: State Department (passport photo).

---

# Contents

---

<b>Letter</b>		<b>1</b>
	Results in Brief	3
	Background	6
	New Passports and Visas Have Been Enhanced, but Prior Generations of Travel Documents Remain More Vulnerable to Fraud, and Document Designs Are Not Periodically Reassessed	13
	Steps Taken to Secure Passports and Visas in the Issuance Process, but Additional Measures Are Needed to Address Weaknesses in Oversight of Passport Acceptance Facilities	23
	Limitations in Technology and Training Affect Inspection Officers' Ability to Fully Utilize Security Features in Passports and Visas	32
	Conclusions	42
	Recommendations for Executive Action	43
	Agency Comments and Our Evaluation	44
<b>Appendix I</b>	<b>Scope and Methodology</b>	<b>46</b>
<b>Appendix II</b>	<b>Types of Passports</b>	<b>49</b>
<b>Appendix III</b>	<b>Testing Conducted in Development of E-Passport Design</b>	<b>50</b>
<b>Appendix IV</b>	<b>Issuance Process for Passports and Visas</b>	<b>51</b>
	Passport Issuance Process	51
	Visa Issuance Process	52
<b>Appendix V</b>	<b>Primary Inspection Processes at Air, Sea, and Land Ports of Entry</b>	<b>54</b>
<b>Appendix VI</b>	<b>Comments from the Department of State</b>	<b>58</b>
	GAO Comments	67

---

<b>Appendix VII</b>	<b>Comments from the Department of Homeland Security</b>	69
	GAO Comment	72

---

<b>Appendix VIII</b>	<b>GAO Contact and Staff Acknowledgments</b>	73
----------------------	--	----

---

**Tables**

Table 1: Number of Fraudulent U.S. Passports and Visas Detected at U.S. Ports of Entry, Fiscal Year 2006	10
Table 2: Validity Period and Numbers in Circulation, by Passport	14
Table 3: Validity Period and Numbers in Circulation, by Visa	16

---

**Figures**

Figure 1: Key Elements of a Secure Travel Document	8
Figure 2: Timeline for Development of E-Passport	19
Figure 3: Timeline for Development of Lincoln Visa	20
Figure 4: Overview of the Process, Tools, and Technology for Primary Inspection of Travel Documents at U.S. Air, Sea, and Land Ports of Entry	34
Figure 5: Overview of US-VISIT Procedures at Air, Sea, and Land Ports of Entry	36
Figure 6: Overview of the Process, Tools, and Technology for Secondary Inspection of Travel Documents at U.S. Ports of Entry	39
Figure 7: Application and Issuance Process for Passports	52
Figure 8: Application and Issuance Process for Visas	53
Figure 9: Inspection Process for Entry into the United States	55

---

---

## Abbreviations

APIS	Advanced Passenger Information System
BCC	border crossing card
CBP	U.S. Customs and Border Protection
CCD	Consular Consolidated Database
DHS	Department of Homeland Security
FDL	Forensic Document Laboratory
GPO	Government Printing Office
ICAO	International Civil Aviation Organization
NIST	National Institute of Standards and Technology
PIERS	Passport Information Electronic Retrieval System
RFID	radio frequency identification
TECS	Treasury Enforcement Communications System
US-VISIT	U.S. Visitor and Immigrant Status Indicator Technology
USCIS	U.S. Citizenship and Immigration Services

This is a work of the U.S. government and is not subject to copyright protection in the United States. It may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



United States Government Accountability Office  
Washington, DC 20548

---

July 31, 2007

The Honorable Lamar S. Smith  
Ranking Member  
Committee on the Judiciary  
House of Representatives

The Honorable Ileana Ros-Lehtinen  
Ranking Member  
Committee on Foreign Affairs  
House of Representatives

The Honorable Darrell Issa  
The Honorable F. James Sensenbrenner Jr.  
House of Representatives

U.S. travel documents are often used fraudulently in connection with other crimes, including narcotics trafficking, alien smuggling, and even terrorism. In fiscal year 2006, more than 21,000 fraudulent U.S. passports and U.S. visas<sup>1</sup> were intercepted by U.S. Customs and Border Protection (CBP) at U.S. ports of entry,<sup>2</sup> and over 3,500 new cases of passport and visa fraud, including application fraud, were investigated by the State Department (State) in fiscal year 2005, resulting in the arrests of over 500 people. Preventing, detecting, and responding to the fraudulent use of passports and visas is essential to protect U.S. citizens and interests at home and abroad. The integrity of these travel documents is dependent upon the combination of security features in the document and solid issuance and inspection processes. State's Bureau of Consular Affairs issues passports and visas, CBP, in the Department of Homeland Security (DHS), inspects these documents at ports of entry, and State's Bureau of Diplomatic Security together with State's Office of the Inspector General are responsible for investigating passport or visa fraud.

---

<sup>1</sup>In this report, we use "passport" to refer to passports issued to U.S. citizens and "visa" to refer to immigrant and nonimmigrant visas issued to foreign nationals seeking to travel to the United States.

<sup>2</sup>A port of entry is an officially designated location (airport, seaport, and land border locations) where CBP officers clear travelers for entry into the United States. There are 326 ports of entry.

---

In response to your request, this report focuses on travel documents issued by State, including passports, passport cards,<sup>3</sup> visas, and border crossing cards (BCC);<sup>4</sup> it examines (1) fraud prevention features in the documents, the process for addressing potential risks, and how information on these features is shared; (2) the integrity of the issuance process; and (3) how these documents are inspected at U.S. ports of entry. We will be issuing a separate report on the security of travel documents issued by DHS in early 2008.

To examine the fraud prevention features in passports and visas, the process for addressing potential risks, and how information on these features is shared, we reviewed documentation on passports and visas, including materials on their security features, available counterfeit deterrence and durability studies, fraud bulletins and alerts, and relevant laws and regulations. We interviewed officials at State's Bureau of Consular Affairs and Diplomatic Security, DHS's Forensic Document Laboratory (FDL), Department of Commerce's National Institute of Standards and Technology (NIST), and the U.S. Government Printing Office (GPO). We also attended the International Civil Aviation Organization (ICAO) machine-readable travel document symposium in Montreal, Canada. To examine the integrity of the issuance process for these documents, we reviewed documentation, including reports and audits of internal controls, production and issuance procedures, and passport fraud referral statistics. We also interviewed officials at State's Consular Affairs Bureau, GPO, and DHS's U.S. Citizenship and Immigration Services (USCIS) and interviewed officials at seven domestic passport offices, two U.S. consulates in Mexico, and two USCIS production facilities. To examine how these documents are inspected at U.S. ports of entry, we reviewed various documents, including CBP inspections program policies, procedures, and related memorandums and relevant laws and regulations. We interviewed officials at CBP, FDL, and the U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program. We also conducted nine site visits to air, land, and sea ports of entry to interview CBP officials and observe the inspection process of passports and visas. Appendix I contains additional details on our scope

---

<sup>3</sup>The passport card is currently under development as an alternative travel document for entry by U.S. citizens into the United States at land and sea ports of entry.

<sup>4</sup>The State Department issues the BCC, which permits limited travel by Mexican citizens, without additional documentation 25 miles inside the border of the United States (75 miles if entering through certain ports of entry in Arizona) for fewer than 30 days.

---

and methodology. We conducted our review from June 2006 through May 2007 in accordance with generally accepted government auditing standards.

---

## Results in Brief

State has developed passports and visas that are more secure than older versions of these documents because they contain a variety of enhanced security features that, in combination, are intended to deter alteration or counterfeit attempts. Prior generations of these documents have been fraudulently used and remain more vulnerable to fraud for the duration of their life span. For example, the 1994 generation of the passport—issued until 2001 and valid for travel until 2011—remains vulnerable to alteration by such means as photo substitution. More than 20 million of these older passports are in circulation. State has made enhancements to strengthen new generations of passports and visas, changing the design of these documents in response, in part, to detected attempts to counterfeit or alter these documents. Although State has updated or changed the security features of its travel documents, it does not have a structured process—such as long-term or “life-span” planning—to periodically reassess the effectiveness of the documents’ security features against evolving threats and to plan for new generations of travel documents. Moreover, the process for designing a new document takes several years. Given the long validity period of these documents and the time it takes to complete a new document design, a structured process for periodically reassessing documents currently issued is critical to ensuring the security of these documents against evolving fraudulent threats.

While State has taken several measures to ensure the security of its travel documents, additional measures are needed in the passport issuance process to minimize the risk of fraud. About 8,500 passport acceptance facilities nationwide serve an important function in establishing the identity (identifying a match between the individual, identification document, and submitted application photo) for millions of passport applicants each year—a vital link in preventing the issuance of genuine passports to criminals or terrorists under false identities resulting from the receipt of a fraudulent application. We found that State lacks a program for oversight of these passport acceptance facilities nationwide. Although State has taken some steps to address weaknesses identified in the training of acceptance agents, additional measures are needed to ensure adequate controls over the application acceptance process. For example, although State officials told us there have been some cases of fraud associated with passport acceptance facilities or the individuals working at these facilities, there is no national system for conducting routine audits



---

of acceptance facilities' performance and practices. Oversight of the acceptance facility program is critical to ensure adequate controls over the application acceptance process and to protect against vulnerabilities, such as the issuance of passports to criminals or terrorists under false identities. For visas issued by State to foreigners seeking to travel to the United States, State has made improvements to the visa issuance process in the last several years and is working to address identified weaknesses. For example, State has taken actions to improve internal controls over visa issuance in response to our and State Inspector General reviews, and it acknowledges that these actions require constant vigilance. In addition, to address the high imposter fraud associated with the BCC, State has recently implemented measures to secure this travel document.

Officers in primary inspection—the first and most critical opportunity at U.S. ports of entry to identify individuals seeking to enter the United States with fraudulent travel documents—are unable to take full advantage of the security features in passports and visas due to (1) limited availability or use of technology at primary inspection and (2) lack of timely and recurring training on the security features and fraudulent trends for passports and visas. These officers rely on both their observation of travelers and visual and manual examination of documents to detect fraudulent passports and visas. However, DHS has not yet provided most ports of entry with the technology tools that can make use of the electronic chips in electronic passports.<sup>5</sup> Further, CBP does not have a process in place for primary inspection officers to utilize the fingerprint features of visa holders, including BCCs, at all land ports of entry. For example, although BCC imposter fraud is high, primary officers at southern land ports of entry are not able to use the available fingerprint records of BCC holders to confirm the identity of travelers and do not routinely refer BCC holders to secondary inspection, where officers do have the capability to utilize fingerprint records. As a result, the officers must rely on other inspection techniques to detect BCC imposter fraud. Moreover, training materials provided to officers were not updated to include exemplars—genuine documents used for training purposes—of the e-passport and the emergency passport in advance of the issuance of these documents. As a consequence, inspection officers were not familiar

---

<sup>5</sup>DHS deployed e-passport readers to meet its legislative requirements under the Visa Waiver Program. The 33 airports to which the readers were deployed process the highest volume of travelers from Visa Waiver Program countries. Citizens of countries participating in the Visa Waiver Program are not required to obtain a U.S. visa to enter the United States for business or tourist purposes for 90 or fewer days.

---

with the look and feel of security features in these new documents before inspecting them. Without updated and ongoing training on fraudulent document detection, officers told us they felt less prepared to understand the security features and fraud trends associated with all valid generations of passports and visas. Although CBP faces an extensive workload at many ports of entry and has resource constraints, there are opportunities to do more to utilize the security features in passports and visas during the inspection process to detect their fraudulent use.

We are making recommendations to the Secretary of State to better plan for the new generations of travel documents and address vulnerabilities in the passport application process. We also are making recommendations to the Secretary of Homeland Security to make better use of the security features in passports and visas in the inspection process and improve training for inspection officers on the features and fraud trends for these travel documents. Specifically, we are recommending that

- State develop a process and schedule for periodically reassessing security features in the design of its travel documents;
- State establish a formal oversight program of passport acceptance facilities;
- DHS develop a deployment schedule for providing e-passport readers to U.S. ports of entry;
- DHS develop a strategy for better utilizing the biometric features of the BCCs in the inspection process; and
- DHS and State identify a process for updating training materials for inspection officers that reflect changes in passports and visas in advance of issuance, including the provision of exemplars of the new documents prior to issuance.

We provided a draft of this report to the Departments of State and Homeland Security, U.S. Government Printing Office, and the Department of Commerce's National Institute of Standards and Technology. We received written comments from State and DHS, which we have reprinted in appendixes VI and VII, respectively. GPO and NIST provided technical comments. State and DHS concurred with the findings and recommendations of the report. State agreed with our recommendations and described the actions it is taking and plans to take to implement them. State also provided additional information on the Consular Consolidated

---

Database (CCD), recent visa fraud cases, and the ways in which State identifies fraudulent passports and visas. DHS concurred with all of our recommendations and described the actions it is taking and plans to take to implement them. DHS believes it has already implemented our recommendation that it develop a strategy for better utilizing the biometric features of BCCs in the inspection process. We agree that DHS's US-VISIT capability enables primary inspectors at air and most sea ports of entry to use fingerprint biometrics to compare and authenticate the document and holder of visas and BCCs. However, at land border ports this capability is not available in primary inspection. Travelers with BCCs at southern land border ports—the ports where BCC imposter fraud is most significant—are not routinely referred to secondary inspection, where they do have the capability to utilize the fingerprint records for comparison, and all BCCs are not machine-read for access to the biographic data during inspection at these ports of entry. As a result, inspectors are not making full use of the biometric information available for BCCs. To more fully utilize the available fingerprint biometric in the BCC and mitigate imposter fraud, we are suggesting that DHS develop a strategy to better use both the fingerprint biometric of the BCC and increase card reads of the BCC in primary inspection at southern land border ports of entry. State and DHS also provided technical comments, which we incorporated, as appropriate.

---

## Background

Travelers to the United States are generally required to present documentation verifying their identity and nationality and, for non-U.S. citizens, their eligibility to enter the United States. Acceptable travel documents for entry into the United States include, among others, passports, visas, and U.S. military identity cards. In 2004, Congress, in an effort to further secure U.S. borders, mandated the development and implementation of a plan that requires U.S. citizens to have a passport or other document that demonstrates their identity and citizenship when entering the United States. State and DHS implemented this requirement

---

for air ports of entry on January 23, 2007, and are to implement the requirement for land and sea ports before June 1, 2009.<sup>6</sup>

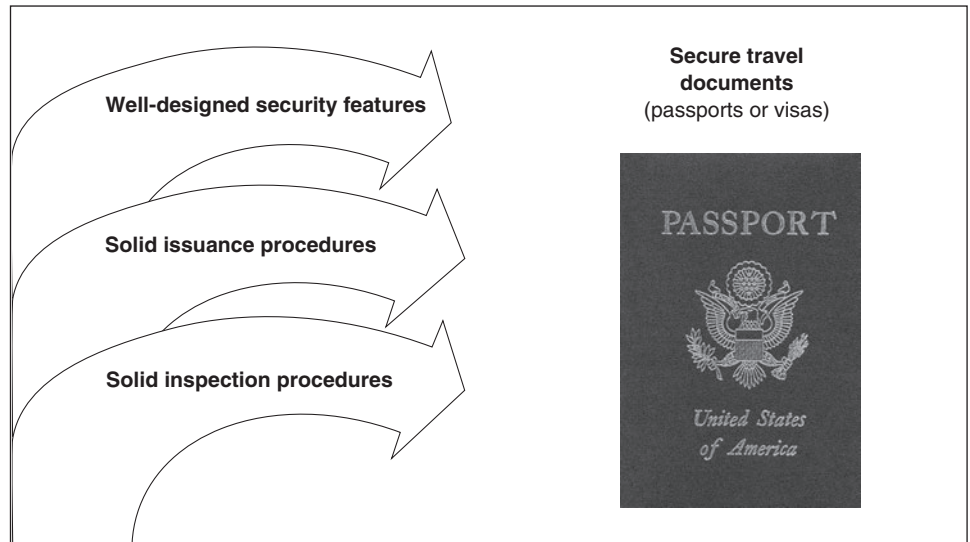
State's Bureau of Consular Affairs is responsible for the design and issuance of passports for U.S. citizens and visas for all foreign aliens requiring a visa for entry into the United States. CBP is responsible for inspecting these documents and permitting entry to travelers at designated air, land, and sea U.S. ports of entry. In addition, State's Bureau of Diplomatic Security, in collaboration with State's Office of Inspector General, DHS and other U.S. agencies, and foreign law enforcement entities, is responsible for investigating suspected fraud of passports and visas.

The security of passports and visas and the ability to prevent and detect their fraudulent use are dependent upon a combination of well-designed security features, solid issuance procedures for the production of the document and review of the application, and solid inspection procedures that utilize available security features. Figure 1 below presents the key elements of a secure travel document. A well-designed document has limited utility if it is not well-produced or inspectors do not utilize the security features to verify the authenticity of the document and its bearer.

---

<sup>6</sup>On June 8, 2007, State and DHS announced that U.S. citizens traveling to Canada, Mexico, the Caribbean, and Bermuda who have applied for but not yet received passports can nevertheless temporarily enter and depart from the United States by air with a government-issued photo identification and Department of State official proof of application for a passport through September 30, 2007. DHS and State have indicated that they will begin to implement the requirement for land and sea ports in 2008. In commenting on a draft of this report, State noted that the exact implementation date will be determined by a number of factors, including the progress of DHS and State actions to implement the Western Hemisphere Travel Initiative and the availability of compliant documents on both sides of the border.

**Figure 1: Key Elements of a Secure Travel Document**



Source: State Department (passport photo).

## Travel Documents Issued by State

In fiscal year 2006, about 12 million passports and almost 6 million visas were issued, according to State. As of April 2007, there are 74 million valid passports and almost 34 million visas, including 9 million BCCs, in circulation.

### Passports

A passport is not only a travel document required of U.S. citizens for international travel and re-entry into the United States by air, but also an official verification of the bearer's origin, identity, and nationality. Under U.S. law, the Secretary of State has the authority to issue passports, which may be valid for up to 10 years. Only U.S. nationals may obtain a U.S. passport, and evidence of citizenship or nationality is required with every passport application. Federal regulations list those who do not qualify for a passport, including those who are subjects of a federal felony arrest warrant. See appendix II for additional information on the types of U.S. passports.

---

In addition, State is currently developing a passport card that will serve as an alternative travel document for re-entry into the United States by U.S. citizens at land and sea ports of entry.<sup>7</sup>

## Visas

A visa is a travel document for people seeking to travel to the United States for a specific purpose, including to immigrate, study, visit, or conduct business; the document allows a person to travel to a United States port of entry and ask for permission to enter the country. While consular officers within State are responsible for determining a person's eligibility to enter the United States for a specific purpose, CBP officers have the ultimate authority to permit entry into the United States. State issues two types of visas: (1) a visa foil attached to the visa pages of a foreign passport, for nonimmigrant or immigrant travel to the United States; and (2) the BCC for limited travel by Mexican citizens within the United States' southern border. Visas can be issued for a validity period of up to 10 years.

---

## Passports and Visa Fraud

Threats to the security of travel documents include counterfeiting a complete travel document, construction of a fraudulent document, photo substitution, deletion or alteration of text, removal and substitution of pages, theft of genuine blank documents, and assumed identity by imposters. Features of travel documents are assessed by their capacity to secure a travel document against the following:

- counterfeiting: unauthorized construction or reproduction of a travel document.
- forgery: fraudulent alteration of a travel document.
- imposters: use of a legitimate travel document by people falsely representing themselves as legitimate document holders.

Most reported passport and visa fraud is imposter-related fraud. In fiscal year 2006, CBP detected 21,292 fraudulent U.S. passports, visas, and BCCs presented by travelers attempting to enter the United States through a U.S. port of entry. (See table 1.) Nearly 80 percent of these documents were

---

<sup>7</sup>The passport card is being developed as a substitute for a passport and as a lower-cost means of establishing identity and nationality for American citizens, as a part of the Western Hemisphere Travel Initiative. This document is not designed to be a globally interoperable travel document as defined by ICAO.

genuine documents presented by imposters. The most frequent fraudulent attempts were by imposters attempting to use a legitimate BCC, while the fraudulent use of passport and visa more often involved attempts to counterfeit or alter the document. The following cases illustrate attempts to fraudulently use U.S. travel documents to enter the United States:

- In November 2005, CBP officers intercepted a Ghanaian citizen with an altered U.S. visa. The visa photo was manually retouched to bear closer resemblance to the photo substituted into the biographical page of the passport.
- In June 2006, a Chinese citizen was found in possession of a counterfeit U.S. passport. Printing and other errors on the biographic page and another page alerted authorities that the passport was counterfeit.
- In January 2007, a Brazilian citizen, using a genuine U.S. visa, attempted to enter the United States as an imposter. CBP officers confirmed the traveler was an imposter and was attempting to enter the United States to seek employment.

**Table 1: Number of Fraudulent U.S. Passports and Visas Detected at U.S. Ports of Entry, Fiscal Year 2006**

Travel document	Imposter	Counterfeit/altered	Total
U.S. passport	971	458	<b>1,429</b>
U.S. nonimmigrant visa foil	173	2,865	<b>3,038</b>
BCC	15,911	914	<b>16,825</b>
<b>Total</b>	<b>17,055</b>	<b>4,237</b>	<b>21,292</b>

Source: GAO analysis of Department of Homeland Security data.

Note: Data for U.S. immigrant visas not available.

Applicants commit passport application fraud through various means, including submitting false claims of lost, stolen, or mutilated passports; child substitution; and counterfeit citizenship documents. According to State’s Bureau of Diplomatic Security investigators, imposters’ use of assumed identities, supported by genuine but fraudulently obtained identification documents, is a common and successful way to fraudulently obtain a passport. This method accounted for about 65 percent of 3,703 total confirmed passport fraud cases investigated by the bureau in fiscal year 2006, according to Diplomatic Security documentation.

---

## Document Security Features

To combat document fraud, security features are used in a wide variety of documents, including currency, identification documents, and bank checks. Security features are used to prevent or deter the fraudulent alteration or counterfeiting of such documents. In some cases, an altered or counterfeit document can be detected because it does not have the look and feel of a genuine document. For instance, detailed designs and figures are often used on documents with specific fonts and colors. While such aspects are not specifically designed to prevent the use of altered or counterfeit documents, inspectors can often use them to identify nongenuine documents. In some cases, security features can be observed with the naked eye. But for others, tools may be necessary to verify the existence of a security feature. For instance, to read microprinting, it may be necessary to have a magnifying glass or a loupe. To see features on pages printed with ultraviolet fluorescent ink, it is necessary to have an ultraviolet light source. In particular, electronic equipment is required to read electronic features such as biometrics or digital signatures from the travel document.

While security features can be assessed by their individual ability to help prevent the fraudulent use of the document, it is more useful to consider the entire document design and how all of the security features help to accomplish this task. Layered security features tend to provide better document security by minimizing the risk that the compromise of any individual feature of the document will allow for the unfettered fraudulent use of the document. Individual document security features are known to different levels of people. For instance, some security features are known only by forensic examiners, while other features are more widely known by specialized law enforcement personnel.

---

## Passport Application and Issuance Process

GPO produces and delivers blank passports to the domestic passport-issuing offices.<sup>8</sup> State operates 17 domestic passport-issuing offices, where most passports are issued each year.<sup>9</sup> In addition, in the spring of 2007, State opened a new passport production facility for the personalization of

---

<sup>8</sup>GPO produces blank passports for State as agreed under a memorandum of understanding with State.

<sup>9</sup>State operates passport-issuing offices in Aurora, Colorado; Boston; Charleston, South Carolina; Chicago; Honolulu; Houston; Los Angeles; Miami; New Orleans; New York; Norwalk, Connecticut; Philadelphia; Portsmouth, New Hampshire; San Francisco; Seattle; and two offices in Washington, D.C.—a regional passport agency and a special issuance agency that handles official U.S. government and diplomatic passports.



---

passport books.<sup>10</sup> The majority of passport applications are submitted by mail or in person at one of 8,500 passport application acceptance facilities nationwide, which include post offices; federal, state and probate courts; public libraries; and county and municipal offices.<sup>11</sup> The passport acceptance agents at these facilities are responsible for, among other things, verifying whether an applicant's identification document, such as a driver's license, actually matches the applicant. Then, at the domestic passport-issuing offices, passport examiners determine—through a process called adjudication—whether they should issue each applicant a passport. See appendix IV for an overview of the passport issuance process.

---

## Visa Application and Issuance Process

State manages the visa process, as well as the consular officer corps and its functions at 219 visa-issuing posts overseas. The process for determining who will be issued or refused a visa contains several steps, including documentation reviews, in-person interviews, collection of biometrics (facial image and fingerprints), and cross-referencing an applicant's name against the Consular Lookout and Support System (CLASS)—State's name-check database that posts use to access critical information for visa adjudication. In some cases, a consular officer may determine the need for a Security Advisory Opinion, which is information provided from Washington to the post regarding whether to issue a visa to the applicant. See appendix IV for an overview of the visa issuance process.

---

## Passport and Visa Inspection Process

In general, at ports of entry, travelers seeking admission to the United States must present themselves and a valid travel document, such as a passport or a U.S. visa,<sup>12</sup> for inspection to a CBP officer. The immigration-related portion of the inspections process requires the officer to determine—by questioning the individual and inspecting the travel

---

<sup>10</sup>While the majority of passports are issued by domestic passport agencies, consular officers in U.S. embassies and consulates also issue passports in the form of an emergency passport.

<sup>11</sup>This number is as of April 2007. State officials noted that this number changes frequently as new acceptance facilities are added and others are dropped.

<sup>12</sup>Currently, U.S. citizens are not required to present passports if they re-enter the United States at a land or sea port of entry. In general, aliens must present their passport and a valid U.S. visa.

---

documents—if the traveler is a U.S. citizen or alien. If the traveler is an alien, CBP officers must determine the purpose of the individual’s travel and whether the alien is entitled to enter the United States. During the inspections process, CBP officers must confirm the identity and nationality of travelers and determine the validity of their passports and visas by using a variety of inspection techniques and technology.

At the first part of the inspection process—primary inspection—CBP officers inspect travelers and their travel documents to determine if they may be admitted or should be referred for further questioning and document examination. If additional review is necessary, the traveler is referred to secondary inspection—an area away from the primary inspection area—where another officer makes a final determination to admit the traveler or deny admission for reasons such as the presentation of a fraudulent or counterfeit passport or visa. See appendix V for an overview of the inspection process at U.S. ports of entry.

---

## New Passports and Visas Have Been Enhanced, but Prior Generations of Travel Documents Remain More Vulnerable to Fraud, and Document Designs Are Not Periodically Reassessed

State has made enhancements to strengthen new generations of passports and visas, which contain a variety of security features that, in combination, are intended to deter attempts to alter or counterfeit the documents; however, prior generations of these documents have been fraudulently used and remain more vulnerable to fraudulent attempts for the duration of their life span. While the process for designing a new document takes several years to complete, State does not periodically reassess the security features of the travel documents it currently issues to identify their effectiveness against evolving counterfeit and alteration threats and to plan for new generations of travel documents. In addition, State shares information on the security features of passports and visas with domestic and international entities.

---

## New Generations of Passports and Visas Have Enhanced Security Features, but Older Versions Are Susceptible to Fraud

Passports and visas contain a variety of security features that, in combination, are intended to deter attempts to alter or counterfeit the documents. The design of passports—currently there are three generations valid for travel—contain a range of security features to protect against their fraudulent use. Visa foils—currently there are two generations valid for travel—and the BCC also contain a range of security features to protect against their fraudulent use. Enhancements have been made to strengthen new generations of these documents, but prior generations remain more vulnerable to fraudulent attempts during their

life span. Although none of the passports and visas that are currently valid have had all of their security features compromised, some methods of alteration or counterfeiting have been found to be successful enough to fool an initial inspection. In these cases of sophisticated attempts to defeat specific security features, only a more detailed examination of the document can determine that the document is not authentic.

## Security Features of Passports

According to State, over 74 million passports are currently in circulation, as of April 2007. Currently, there are three valid generations of the passport—the 1994 passport, the 1998 photo-digitized passport, and the 2006 electronic passport (e-passport). See table 2 for validity periods for travel and numbers in circulation of current passports.

**Table 2: Validity Period and Numbers in Circulation, by Passport**

U.S. passport	First issued	Last issued	Valid for travel <sup>a</sup>	Number in circulation (as of April 2007)
1994 passport	1994	2001	through 2011	20 million
1998 photo-digitized passport	1998	2007 <sup>b</sup>	through 2017	52 million
e-passport	2005	Currently issued	through 2017 or later	2 million or later

Source: State Department.

Notes:

About 140,000 passports were issued to U.S. citizens living overseas prior to April 2002 or as an emergency passport prior to August 2006. After April 8, 2002, overseas passport issuance for U.S. citizens residing or traveling abroad was transferred to the National Passport Center in Portsmouth, New Hampshire, and the Charleston Passport Center in Charleston, South Carolina, except for those requiring urgent travel. All passports issued to U.S. citizens living overseas are adjudicated by consular officers at U.S. embassies and consulates.

<sup>a</sup>Only for passports issued with a 10-year validity period in the last issuance year.

<sup>b</sup>State is issuing the 1998 passport until the inventory supply of these books is diminished, which State expects will occur in August 2007.

Each generation of the passport has a range of security features to provide protection against the threat of fraudulent use. As each generation of passports is developed, some security features are enhanced, others added, and others dropped from the documents' design to protect against counterfeit and alteration threats. For example, photo substitution, particularly with the 1994 passport, is one technique that has been used to alter passports. State has enhanced subsequent generations to combat this threat. In the 1998 passport, State enhanced the laminate of the passport and introduced a photo-digitized passport that prints scanned photographs

---

on the biographic page of the passport to eliminate the possibility of individuals cutting out and replacing the laminated photos. While the vulnerability to photo substitutions has been reduced in the 1998 passport, it has not been fully eliminated. For the e-passport, although State continues to print the photos in the same way as the prior generation, additional enhancements have been made to the security of the laminate and a proximity radio frequency identification (RFID) chip has been added that provides for electronic storage of biographical and biometric data.<sup>13</sup> The information stored on the chip is protected by a digital signature.<sup>14</sup> This enhancement, which allows for a comparison of the photo in the passport with the photo in the chip, can provide greater assurance that the photo, as well as the biographic data, has not been altered or counterfeited. In cases where these enhancements may fail to work correctly, it is important to plan for the potential failure of equipment or incidents where the verification system does not correctly match individuals. In addition, the proposed passport card is expected to include laser engraving, tactile features in the photo area and an optically variable device to address photo substitution techniques. Additional information on the security features in passports and visas issued by the State Department are sensitive in nature and have not been provided in this report. We will be reporting on the security features in these documents in a separate report.

## Security Features of Visas

According to State, over 34 million visas are in circulation as of April 2007. Currently, there are two valid generations of the visa foil—the Teslin and the Lincoln—the foil is attached inside a foreign passport using an adhesive.<sup>15</sup> The only currently valid generation of the BCC—issued to Mexican citizens—is the laser visa, a polycarbonate card with an optical

---

<sup>13</sup>Technologies called biometrics can automate the identification of individual travelers by one or more of their distinct physical or behavioral characteristics. For more information on biometrics, see GAO, *Technology Assessment: Using Biometrics for Border Security*, [GAO-03-174](#) (Washington, D.C.: Nov. 14, 2002).

<sup>14</sup>A document or file may be protected using a cryptographic process that effectively generates a “digital signature” stored in the document. Validating the digital signature not only confirms who generates it, but also ensures that there have been no alterations to the document since it was signed. For more information about digital signature technology, see GAO, *Information Security: Advances and Remaining Challenges to Adoption of Public Key Infrastructure Technology*, [GAO-01-277](#) (Washington, D.C.: Feb. 26, 2001).

<sup>15</sup>The Teslin visa used a Teslin synthetic substrate, while the Lincoln visa, so named because of the image of President Lincoln on the visa, is made of paper.

stripe to electronically store information about the BCC holder.<sup>16</sup> See table 3 for data on validity periods for travel and numbers in circulation of current visas.

**Table 3: Validity Period and Numbers in Circulation, by Visa**

U.S. visa	First issued	Status	Valid for travel <sup>a</sup>	Number in circulation (as of April 2007)
Teslin visa <sup>b</sup>	1993	Last issued 2003	through 2013	11 million
Lincoln visa	2002	Currently issued	through 2017 or later	14 million
BCC	1998	Currently issued	through 2017 or later	9 million

Source: State Department.

<sup>a</sup>Only for visas issued with a 10-year validity period in the last year of issuance.

<sup>b</sup>There are three versions of the Teslin visa—type 1, type 2, and the machine-readable visa 2000 (MRV2000).

As with the passport, when the Lincoln visa was developed, some security features were improved over those in the Teslin visa, others added, and others dropped. Enhancements to the Lincoln visa include more detailed printing features and features such as security fibers and biometric information (digital photograph and fingerprints). The biometric information is collected overseas under State’s Biometric Visa Program, to be used by CBP inspectors at ports of entry to verify that the original visa applicant is the person entering the United States.<sup>17</sup> For the BCC, State stored the traveler’s biographical and biometric information electronically on the optical media of the card.

<sup>16</sup>The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), as amended, mandated the expiration of previous versions of the BCC on September 30, 2001.

<sup>17</sup>State implemented the Biometric Visa Program in October 2004.

---

## Although Design Development Requires Years to Complete, State Does Not Periodically Plan for New Generations of Passports and Visas

State's process for the development and testing of new travel documents, to enhance their security and reduce vulnerability to sophisticated fraud attempts, varied by document and required several years to complete. While State has made adjustments in the design of passports and visas, its approach has been largely reactive. Despite the length of time required of a document redesign, State does not have a structured process to periodically reassess the security features in its documents and to plan for new generations. The increasing pace of technological change and use of electronics makes State's current approach less viable than it might have been in the past, and best practices in currency design, for example, suggest that periodic evaluation of designs and introduction of new security features are more viable approaches in the management of counterfeit and alteration threats.

## Development Process for the E-Passport

The process for developing the new e-passport design took almost 3 years. State initiated the redesign of the passport in 2003 in response to new international specifications for electronic travel documents, to meet standards set for nations that participate in the United States' Visa Waiver Program, and to address sophisticated attempts to compromise the document with additional layers and enhancements of security features.<sup>18</sup> In February 2005, State presented the proposed design for the new passport, which was intended to comply with ICAO standards. From 2005-2006, State, together with GPO, utilized government expertise at FDL and the NIST to test the durability of the book and certain security features of the e-passport and emergency passport. In response to security and privacy concerns regarding the inclusion of RFID chip technology, NIST was also requested to evaluate the passport's skimming vulnerability.<sup>19</sup> Based on the results of NIST's tests, material was added to the front cover and spine of the book to mitigate the threat of skimming. Separately, durability testing conducted at NIST also revealed that some of the security features were adversely affected by humidity. State and GPO reviewed the results of NIST's tests and determined that the overall integrity of the passport remained sufficient and did not make any immediate changes to the design, according to State and GPO officials. A

---

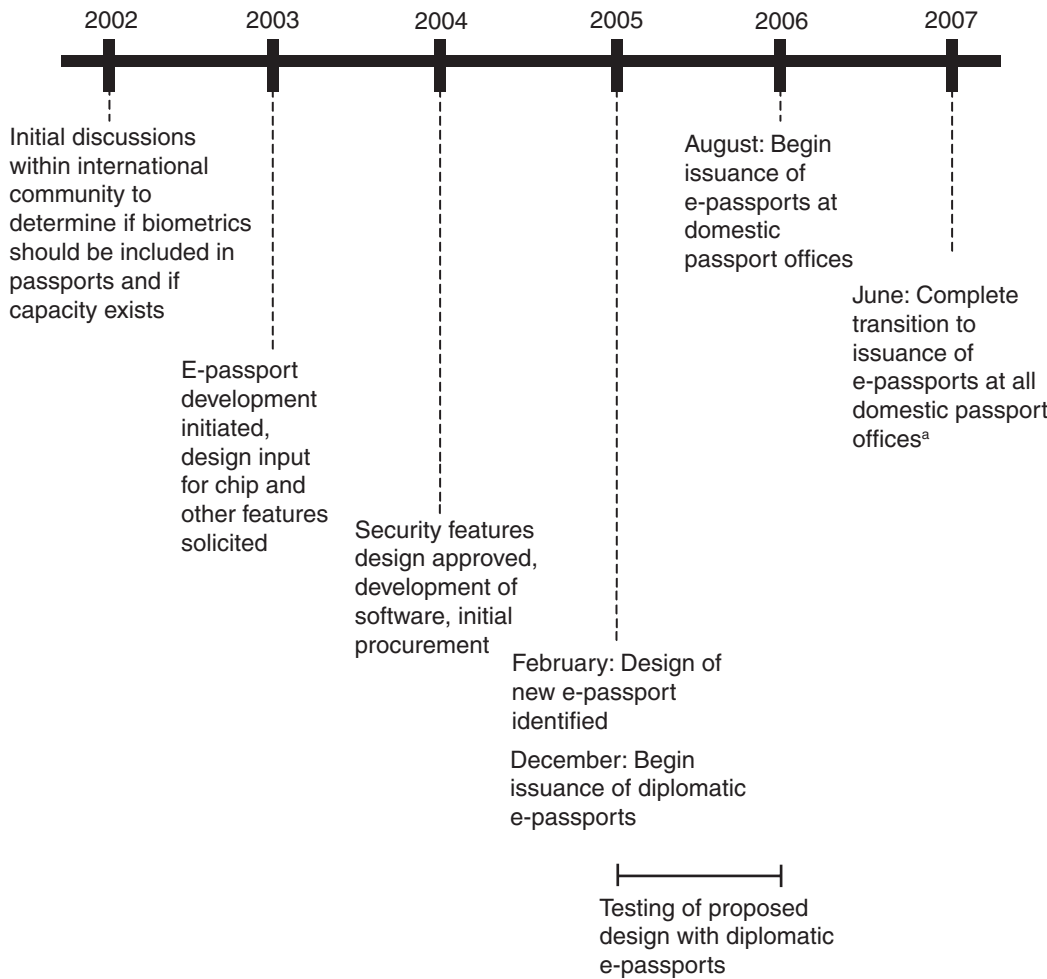
<sup>18</sup>At the same time that the e-passport was under development, the emergency passport was developed to provide U.S. missions overseas, for the first time, with a designated passport book for emergency issuance overseas.

<sup>19</sup>Skimming is the unauthorized use of a reader to read the data stored on the RFID chip without the authorization or knowledge of the owner of the chip or the individual in possession of the chip.

---

State official did note that these results would be considered in the future. In January 2006, State and DHS conducted pilot tests for the new passport, using diplomatic versions of the e-passport. See figure 2 for a timeline of the development process for the e-passport. Appendix III provides additional information on the testing that was conducted in the development of the e-passport design.

**Figure 2: Timeline for Development of E-Passport**



Source: GAO analysis of State Department data.

<sup>a</sup>According to State, all passport agencies and centers have fully converted to e-passport production, but the National Passport Center also continues to print legacy passport books until the inventory supply of these books is diminished, which State expects will occur in August 2007.

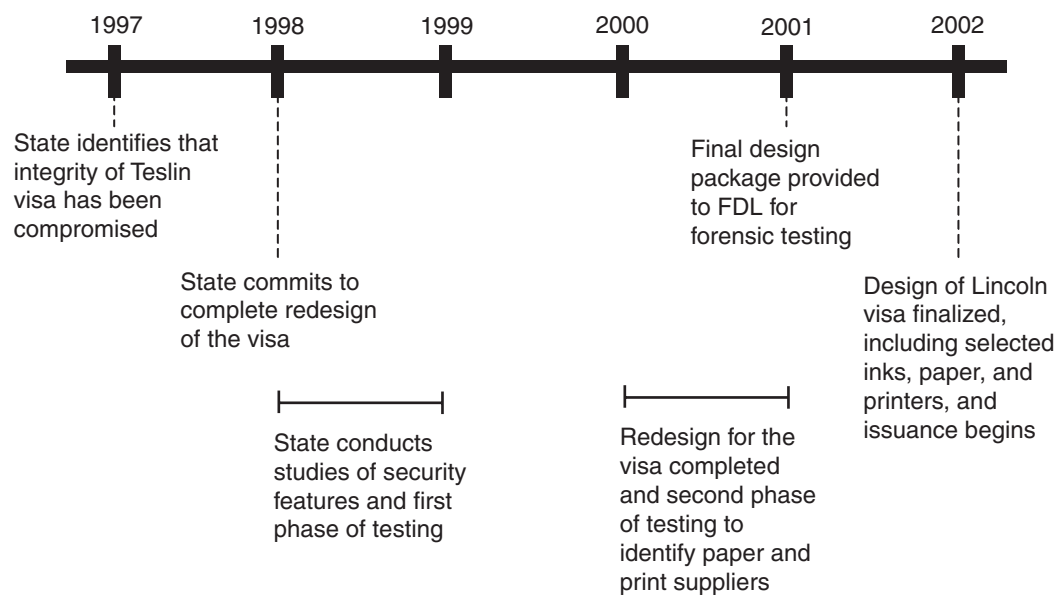
### Development Process for the Lincoln Visa

The development of the Lincoln visa design took about 4 years. The visa was developed in response to advanced attempts to counterfeit and alter the Teslin visa, according to State. To quickly address the sophisticated alteration attempts to the Teslin visa while the Lincoln visa was under development, State developed a new version of the Teslin visa—the MRV-2000—as a short-term solution for addressing the counterfeit threat. The MRV-2000 was tested in 1999 and issued in 2000. State was able to make minor changes on short notice, such as additional coding, to distinguish



the MRV-2000 for inspection purposes and provide a short-term solution during the several years it took for the redesign of the visa to be completed. From 1998 to 1999, State requested industry experts to help in the development of the design and conducted studies of available security papers and ink jet printers. Various paper suppliers and NIST conducted vulnerability tests, demonstrating the durability of features on available papers. According to State officials, after identifying currently advantageous security features, State then moved into the selection of paper, glue, release liner process offset, and florescent inks. FDL provided forensic testing, such as chemical sensitivity testing, for the selected design. See figure 3 for the timeline of development for the Lincoln visa.

**Figure 3: Timeline for Development of Lincoln Visa**



Source: GAO analysis of State Department data.

### Development of Passport Card

The development of the new passport card is expected to take a little more than 2 years, according to current State and DHS plans. State, in consultation with DHS, has been developing a new passport card since early 2006. In January 2006, State and DHS announced the development of the passport card. On May 25, 2007, the solicitation request for proposal for the passport card was released. According to State and DHS plans, from July until December 2007, the proposals will be reviewed and testing will be conducted, including durability testing. State expects to begin issuing the new cards in 2008.

---

State Does Not Have a Structured Process for Periodically Reassessing and Planning for New Generations of Passports and Visas

State updates or changes the security features of its passports and visas in response, in part, (1) to detected attempts to counterfeit or alter these documents and (2) to recommended international standards for secure travel documents. State also made improvements to the passport to match requirements for enhanced security features in the passports from countries in Visa Waiver Program.

State obtains information on the detected attempts to counterfeit or alter passports and visas from a variety of sources in the United States and other nations, according to State officials. For example, State occasionally receives information gathered from DHS regarding the seizures of fraudulent passports and visas. Specifically, FDL provides forensic analysis of identified alterations and counterfeit attempts and CBP's Fraudulent Document Analysis Unit provides trend analysis on the types of fraudulent attempts intercepted at the border. The unit forwards these seized documents—primarily passports—to State, according to Fraudulent Document Analysis Unit and State officials. However, the information that State receives on passport and visa fraud is not centrally collected or analyzed by State for purposes of planning or reassessing the document's security. According to State, information received on the fraudulent use of passports and visas is reviewed largely on a case-specific basis. Moreover, data on this information are not collected or analyzed by State in order to identify counterfeit or alteration trends.

U.S. currency faces threats similar to those of passports and visas. According to the National Academies, life-cycle planning can be an effective way to reassess document security and plan for new documents by providing a structured process for re-evaluating the features of the document against evolving counterfeit and alteration threats.<sup>20</sup> The National Academies found that, for bank notes, advances in reprographic technology have made securing currency more challenging, necessitating regular assessments of technologies and threats. According to the National Academies, by continuously evaluating currency designs and introducing new security features, the government does an effective job of staying ahead of counterfeiting threats. In addition, the U.S. Department of the Treasury's Bureau of Engraving and Printing has reported that protecting U.S. currency is an ongoing process. According to the bureau, it plans to introduce new currency designs every 7 to 10 years.

---

<sup>20</sup>National Academies Press, *Is That Real? Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes*, ISBN-0-309-10124-7 (Washington, D.C., 2006).

---

Although State has recently enhanced some of the security features and introduced new security features to the passport, State, for the documents it issues, does not have a policy for reassessing the design's resistance to evolving counterfeit and alteration threats and planning for new generations of travel documents. For example, although the BCC has been in circulation for almost 10 years, State has not had any formal plans to reassess the current document or develop a new BCC until recently. In responding to a draft copy of this report, State noted that they are currently redesigning the next generation of the BCC for deployment in 2008, when the current BCCs begin to expire.

A structured process for periodically reassessing the security features in documents and planning for new generations should include a policy for reassessing the ability of the document design to resist compromise and fraudulent attempts to the documents. For example, to meet acceptable standards for the use of driver's licenses and identification cards for official purposes, DHS has proposed establishing a policy for annual review of the card design of such documents. This proposed review would address the cards' ability to resist counterfeit and alteration attempts in several areas, including photo substitution, modification of data, duplication, and reproduction, among others. Such a review of the security features in the passport design, such as long-term vulnerability testing of the chip technology and print durability, could identify potential vulnerabilities in these features before they could be exploited.

---

## State Shared Information on Design of Passports and Visas

State shares information on the security features and fraud attempts of passports and visas with U.S. entities, including CBP, FDL, and state and local law enforcement, as well as with State's overseas counterparts, according to agency documents and officials. Specifically, State's Fraud Prevention Program distributes newsletters identifying detected attempts to counterfeit, alter, or fraudulently obtain visas and related fraud to DHS entities and U.S. missions overseas. State also bilaterally shares information on the security features of passports and visas to deter the fraudulent use of these travel documents overseas. For example, State conducts fraud prevention training for host government law enforcement and immigration authorities and also works with host governments on U.S. passport and visa fraud investigations and prosecutions. In addition, State participates in the multilateral organization ICAO to promote travel document security and global interoperability.

While State has shared information on the security features and activities related to the travel documents it issues, including the e-passport, State is

---

only beginning to share information that is necessary to verify the authenticity of the electronic data stored in the chip of the e-passport. The international community, through ICAO, has established a directory for international validation of digital signatures of e-passport chips. The United States is currently taking steps to join the directory and share its public key.

---

## Steps Taken to Secure Passports and Visas in the Issuance Process, but Additional Measures Are Needed to Address Weaknesses in Oversight of Passport Acceptance Facilities

State and GPO have enacted several measures to ensure the security and physical quality of passports and are working to address weaknesses identified in the passport issuance process; however, additional measures are needed to strengthen the process and minimize vulnerabilities. Specifically, State's lack of an oversight program for about 8,500 passport acceptance facilities nationwide continues to present a significant fraud vulnerability. State has made recent improvements to the visa issuance process and is working to address identified weaknesses.

---

## GPO Has Undertaken Measures for Ensuring Physical Security and Quality in Passport Manufacturing Process

GPO has established measures to safeguard the physical security and integrity of the passport book and materials and continues to review and strengthen these measures.<sup>21</sup> In the manufacturing process, GPO has identified measures to secure production materials and blank passport books and to ensure the quality of the books. Specifically, GPO has identified control measures in place for the materials used in the production of passports, including the paper, ink, design, binding, and chip and for the blank books. A 2004 GPO Inspector General security review found vulnerabilities in the physical controls of the blank passport, including the delivery of blank books to passport agencies. GPO has taken steps to improve its internal controls for passport production as a result of this review and other recent GPO Inspector General reviews, according to GPO Inspector General officials. In addition, GPO has established quality assurance measures for the production of the 1998 passport and e-passport to ensure the books are manufactured to proper specifications.

---

<sup>21</sup>GAO's *Standards for Internal Control in the Federal Government* recommends that agencies establish physical controls to secure and safeguard vulnerable assets.

---

For example, GPO staff inspects the quality of the product at stages throughout the manufacturing process, including inspections of the supply materials. GPO has also established procedures to inspect, analyze, and document metrics associated with quality of the passport. In addition, GPO is also instituting an independent inspection entity that will be responsible for conducting unannounced and random inspections at points in the manufacturing process to verify that quality standards are met.

For the e-passport, GPO has identified procedures for inspecting the quality of the chip at several steps along the manufacturing process, while additional measures to further ensure the quality of electronic technology in the e-passport book are under development. According to GPO officials, the established automated system for inspecting the quality of the chip is satisfactory, but the physical quality assurance process is still being developed. Specifically, GPO officials said they are studying international technology standards and lessons learned from international counterparts to develop additional quality assurance procedures for the e-passport manufacturing process.

---

### State Has Established Measures for Ensuring Integrity in the Passport Issuance Process

State has taken several steps to ensure the integrity of the passport throughout the issuance process—including establishing internal control standards, conducting periodic audits and other internal reviews, and establishing quality assurance measures for passport processing.<sup>22</sup> For example, State has identified control measures at its passport offices to safeguard passport applications, passport books, and other production supplies. Specifically, State’s internal controls handbook for domestic passport offices provides guidance for ensuring the integrity of passport operations, including guidance for (1) employee integrity and conduct, (2) applications receipt, (3) counter applications, (4) cashiering, (5) adjudication, (6) blank book control, (7) duty officer program, and (8) protection of the premises and information. According to State officials, the handbook is currently being updated to further strengthen controls and address identified weaknesses. The handbook identifies and

---

<sup>22</sup>GAO’s *Standards for Internal Control in the Federal Government* require that agencies establish internal controls sufficient to ensure that transactions and other significant events are authorized and executed only by persons acting within the scope of their authority. The standards also require that the agencies establish internal controls sufficient to ensure that access to resources and records is limited to authorized individuals and that accountability for their custody and use is assigned and maintained.

---

provides procedures for areas of identified vulnerability, including the accountability of passport books, money, and adjudicative decision making, but it does not include internal controls for the passport-related functions performed at the acceptance facilities.

To ensure compliance with these measures, State conducts periodic management assessments and internal control reviews for each domestic passport office as well as periodic audits and other internal reviews of its passport issuance process. These reviews cover general management, use of facilities, adjudication, customer service, fraud prevention, passport book processing, and internal controls, as well as provide recommendations for the improvement of operations. In addition, State also conducts periodic audits and other internal reviews of its passport issuance process.

- First, the management at the domestic passport offices conducts weekly and biweekly audits of adjudicated applications to review compliance with adjudication guidelines.
- Second, State's passport service management in Washington, D.C., has recently taken steps to conduct periodic validation studies, which are large-scale audits of passport applications, at all passport offices. According to State officials, a pilot validation study was conducted in 2006, reviewing over 20,000 adjudicated applications. These officials indicated that they are currently developing the methodology and implementation plan for future validation studies.
- Third, another management-led effort took place in the summer of 2006, when State's Passport Office convened a number of working groups in Washington, D.C., to improve passport operations and address recommendations raised by prior GAO and State Inspector General reports. Specifically, these working groups focused on areas such as the national fraud prevention program; internal controls; and fraud metrics, statistics, and trend analysis. As a result of the recommendations of these working groups, State's passport management plans to implement several initiatives in the next year to improve overall operations.

State also has measures in place to ensure the quality and accuracy of passports issued to applicants. For example, passports are inspected after the applicant's information has been added to the blank passport book to verify the information has been correctly printed and, for e-passports, stored onto the chip. In addition, each e-passport is tested at the issuing

---

passport agency to ensure that the personalized chip can be read by an e-passport reader.

In addition to the efforts described above, State occasionally modifies the regulations governing passport operations. For example, State revised its regulations in 2001 to require that both parents consent to the issuance of a passport for children under age 14 and, in 2004, further amended the regulation to further require that children under age 14 also appear personally when applying for a passport. These changes were made, in part, to improve State's ability to combat international parental child abduction, but the measures have also helped prevent or deter identity theft-related fraud in passport applications, according to State officials. In commenting on a draft copy of this report, State indicated that these changes were also made to comply with related statutory requirements.

---

## Weaknesses Exist in State's Oversight of Passport Acceptance Facilities

We previously reported that the acceptance agent program was a significant fraud vulnerability.<sup>23</sup> State has addressed some weaknesses identified in the training of acceptance agents; the agents serve a critical role in establishing identity, which is critical to preventing the issuance of genuine passports to criminals or terrorists under false identities as a result of receipt of a fraudulent application. However, we found that many of the problems with the oversight of passport acceptance facilities we identified in 2005 persist. Specifically, State lacks an internal control plan for its acceptance facilities to ensure that effective controls are established and monitored regularly.<sup>24</sup> An internal control plan should identify the roles and responsibilities of all individuals whose work affects internal control; lay out specific control areas; cover risk assessment and mitigation planning; and include monitoring and remediation procedures. Moreover, ICAO guidance for the issuance of travel documents recommends several procedures to combat fraudulent applications, including (1) regular training to individuals who accept applications to increase their awareness of potential fraud risks and (2) processes to ensure random access between the acceptance agent and applicant.

---

<sup>23</sup>GAO, *State Department: Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts*, [GAO-05-477](#) (Washington, D.C.: May 20, 2005).

<sup>24</sup>GAO guidance on internal controls recommends that internal control monitoring assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

---

Numerous passport officials and Diplomatic Security investigators told us that the acceptance agent program remains a significant fraud vulnerability. State passport officials told us there have been investigated fraud cases associated with passport acceptance facilities or the individuals working there; however, they did not provide us with additional information on these cases. Examples of acceptance agent errors that were brought to our attention include important information missing from documentation, such as evidence of birth certificates and parents' affidavits concerning permission for children to travel, as well as photos that were not properly attached to the application. One passport specialist also cited a case where the photo submitted with the application did not match the identity of the applicant. In another example, another passport official told us of a case where an acceptance facility had accepted a passport application for an individual without the person being present and, therefore, did not verify the applicant's identity. In addition, managers at two passport offices said their offices often see the same mistakes multiple times from the same acceptance facility. These problems are of particular concern given the persistent attempts to fraudulently obtain legitimate passports using stolen identity documents.

Although resources and other tools are available to passport examiners at domestic passport offices to verify citizenship evidence and potentially detect false claims of identity, there are a number of indicators in the inspection of applicants that enhance the ability to detect efforts to use a false identity to obtain a genuine passport. Moreover, passport examiners and other officials at passport offices told us it is easier to detect application fraud when interviewing applicants directly at the passport counter. However, the majority of passport applications that passport examiners adjudicate are accepted by individuals at passport acceptance facilities.

State has taken action to address some weaknesses we previously identified with the acceptance facility program. These actions include the following:

- In mid-2006, State began to develop a system to track the names and signatures of authorized acceptance agents, the training status of these agents, and the level of proficiency achieved in the training. According to State officials, this system is expected to be fully implemented by the end of 2007.
- In May 2007, State implemented an online training program for use by nonpostal passport acceptance agents. This program was adapted from a



---

computer-based training program previously developed by State and the U.S. Postal Service to train passport acceptance agents at postal service facilities.

- In the spring of 2007, State began to discuss a system for tracking accepted passport applications by acceptance facility.

In addition, State's Bureau of Consular Affairs is proposing to update and amend some of its passport regulations. These amendments would, among other things, codify the requirement that passport acceptance agents be U.S. citizens, permanent employees, and 18 years or older, and have successfully completed the training as detailed by guidance provided by State. While these requirements are already State policy, the proposed changes would make them formal regulations. In addition, another change would require passport acceptance facilities within the United States to maintain a current listing of all passport acceptance agents. If enforced, these regulations would strengthen the application acceptance process.

State officials attribute problems with applications received through acceptance agents to the limited oversight of acceptance agents. For example, accountability for the number of passport agents authorized to accept passport applications remains unclear. Officials at two passport offices confirmed that their passport offices now maintain records of the names of individuals accepting passport applications at designated acceptance facilities in their region. However, they expressed reservations about relying too heavily on the accuracy of this information given the absence of a program to audit or verify the performance of acceptance agents. In addition, State makes a limited number of oversight visits to acceptance facilities. Primarily due to the large number of acceptance facilities in each passport office region, these offices concentrate their training and oversight visits on acceptance facilities geographically close to the passport office or those acceptance facilities identified to have problems. In the absence of a formal mechanism for monitoring the performance of acceptance agents, officials at two of the passport offices we visited had developed individual systems for tracking the passport acceptance facility or agent with an application detected to be fraudulent by passport examiners.

---

## State Continues to Address Vulnerabilities in the Visa Issuance Process

GPO and State have measures for ensuring the quality of visas, including BCCs. In recent years, State has taken a number of steps to strengthen the visa issuance process, as well as a more recent measure to secure BCCs.

---

## Measures for Ensuring the Security and Quality of Visas and Border Crossing Cards

GPO and State have identified measures to ensure the physical security and quality of visas. GPO has measures in place to secure the production of visa foils manufactured by a vendor. GPO approves the vendor's security control plan and conducts, with State, an on-site inspection of the vendor's facility prior to the award of the contract and sharing of a detailed description of the security features in the visa design, according to GPO. State receives the blank visa foils directly from the vendor using a secured carrier.

For the production of BCCs, DHS's U.S. Citizenship and Immigration Service (USCIS) has established a number of automated checks within the production system to ensure that the cards are produced within specifications. One check is a quality assurance examination of the card to ensure that the photo is clear and the fingerprint image is complete and clear. USCIS has inventory control checks to account for all BCCs and to ensure the information printed onto the BCCs corresponds to the data provided by State. For example, the check would ensure that a male's photograph is matched with the correct gender identification. Personalized cards are delivered to the U.S. consulates in Mexico, where the cards are checked for accuracy and quality before being delivered to the applicants.

## State Has Taken Actions to Improve the Integrity of the Visa Issuance Process

State, along with Congress and the Department of Homeland Security have initiated new policies and procedures since the September 11 attacks to strengthen the security of the visa process, particularly as an antiterrorism tool. Such changes include the following:

- Beginning in fiscal year 2002, State began a 3-year transition to remove visa adjudication functions from consular associates.<sup>25</sup> All nonimmigrant visas must now be adjudicated by commissioned consular officers.<sup>26</sup>

---

<sup>25</sup> Consular associates are U.S. citizens and relatives of U.S. government direct-hire employees overseas who, following a successful completion of the required Basic Consular Course, are hired by the consular section at post. Up until September 30, 2005, consular associates at some posts were allowed to assist consular officers in adjudicating visas.

<sup>26</sup> The Intelligence Reform and Terrorism Prevention Act of 2004 required that consular officers adjudicate visas. See P.L. 108-458. As defined by the State Department, consular officers are generally active Foreign Service officers but may also include commissioned civil service employees or retirees of the Foreign Service.

- 
- Personal interviews are now required for most foreign nationals seeking nonimmigrant visas.<sup>27</sup>
  - As of October 2004, consular officers are required to scan visa applicants' right and left index fingers through the DHS Automated Biometric Identification System before an applicant can receive a visa.<sup>28</sup>

In 2005 we reported that consular officers are receiving clear guidance on the importance of addressing national security concerns through the visa process.<sup>29</sup> In addition, we also reported that State has established clear procedures on visa operations worldwide, as well as management controls to ensure that visas are adjudicated in a consistent manner at each post. State has also increased hiring of consular officers; increased hiring of foreign language proficient Foreign Service officers; revamped consular training with a focus on counterterrorism; strengthened fraud prevention efforts worldwide; and improved consular facilities. In addition, consular officers now have access to more information from intelligence and law enforcement databases when conducting name checks on visa applicants.

In addition, in a separate report in 2005, we found that while State's Bureau of Consular Affairs has a set of internal controls to prevent visa malfeasance, and has taken actions to improve them, these internal controls were not being fully and consistently implemented.<sup>30</sup> State has a program of internal controls for visa issuance detailed in the Foreign Affairs Manual and supplemented by standard operating procedures. Examples include controls to ensure random access between applicants

---

<sup>27</sup>Every alien applying for a nonimmigrant visa who is between the ages of 14 and 79 must submit to an in-person interview with a consular officer unless the interview is waived under certain circumstances by either the consular officer or the Secretary of State. There are also circumstances under which the interview cannot be waived.

<sup>28</sup>The Automated Biometric Identification System is a DHS database that includes some 5 million people who may be ineligible to receive a visa. For example, the Automated Biometric Identification System data include, among other records, FBI information on all known and suspected terrorists, selected wanted persons, and previous criminal histories for individuals from high-risk countries. See GAO, *Border Security: State Department Rollout of Biometric Visas on Schedule, but Guidance Is Lagging*, [GAO-04-1001](#) (Washington, D.C.: Sept. 9, 2004); and [GAO-03-174](#).

<sup>29</sup>GAO, *Border Security: Strengthened Visa Process Would Benefit from Improvements in Staffing and Information Sharing*, [GAO-05-859](#) (Washington, D.C.: Sept. 13, 2005).

<sup>30</sup>GAO, *Border Security: More Emphasis on State Consular Safeguards Could Mitigate Visa Malfeasance Risks*, [GAO-06-115](#) (Washington, D.C.: Oct. 6, 2005).

---

and adjudicators, to minimize the risk of malfeasance; controls for its accountable items; and daily supervisory review of all visa refusals and a sample of visa issuances. As we reported, State has taken a number of steps to strengthen its efforts to protect against malfeasance in the issuance process. For example, to prevent the issuances of nonimmigrant visas to unqualified applicants, Consular Affairs has strengthened its efforts to limit employee access to automated systems that issue visas and has taken steps to ensure that visa applicants cannot predict which officers will interview them. It has also strengthened its criteria for applicants referred by post employees for favorable consideration in obtaining a visa and expedited processing by consular officers. Further, Consular Affairs has increased its emphasis on both headquarters and post supervisory oversight—particularly by ambassadors, deputy chiefs of mission, and principal officers—including by providing training and other tools. It also requires posts to certify in writing annually their compliance with key internal controls. Consular Affairs has issued guidelines on reporting suspicious behavior that may involve malfeasance. It has also enhanced its malfeasance prevention efforts. However, we found some of these controls were not always being followed at the posts we visited in 2005. State officials told us they continue to emphasize the importance of full compliance with internal controls.

In addition, State recently took action to secure BCCs in response to the high number of BCCs reported by Mexican citizens as lost or stolen. State officials felt that the ability to obtain another BCC to replace a reportedly lost or stolen BCC was facilitating imposter fraud. In January 2007, State implemented a policy requiring BCC holders who report their BCC stolen to be issued a subsequent BCC in the form of a visa foil inserted in their passport. As of April 2007, about 131,000 BCCs have been issued in the form of a visa foil, according to State. The visa category is marked on the visa foil, indicating the traveler is traveling to the United States under the restrictions of the BCC. State officials told us that the reports of lost or stolen BCCs dropped significantly following the implementation of this initiative.

---

## Limitations in Technology and Training Affect Inspection Officers' Ability to Fully Utilize Security Features in Passports and Visas

The inspection of U.S. passports and visas at ports of entry is a key element in ensuring the security of these documents. Officers are often faced with limited time to process travelers and rely on both the inspection of select features and their interview of the traveler to detect fraudulent use of passports and visas. Limitations in available technology tools at some ports and a lack of timely and continual information on the security features in these documents affect the inspection officers' ability to fully utilize the security features in passports and visas. Specifically, primary inspection officers are unable to utilize the chip technology in the e-passport to verify document authenticity because e-passport readers are not available at 83 air ports of entry and are not designated for U.S. citizen inspections at 33 other airports of entry. Further, primary officers are not able to utilize the available fingerprint records of BCC holders to verify the authenticity of the documents and travelers at southern land ports of entry, and they also do not routinely refer BCC holders to secondary inspection, where they do have the capability to utilize the fingerprint records. In addition, limited training materials and training opportunities also impede officers' ability to learn of the security features and fraudulent trends associated with new and older generations of passports and visas. For example, in advance of State's issuance of the e-passport and the emergency passport, State did not provide a sufficient quantity of exemplars and CBP did not update its training for all inspection officers to include information on the security features of these new travel documents.

---

## Inspection Officers Rely on Observations of Travelers and Examinations of Documents to Detect Fraud

Primary officers are often faced with limited time to process travelers—especially at ports that have a continuous high volume of traffic—and rely on both the observation of travelers' behavior and the examination of travel documents to detect fraudulent use of passports and visas. Specifically, southern land borders face the largest constraints on inspection time due to the high volume of traffic. Many officers at most ports we visited told us they have detected imposters by observing travelers' demeanor, questioning them regarding their travel, and visually comparing the travelers' identities with the biographic data and photo on the travel document. These officers told us they make limited use of the security features in travel documents because of time constraints and often rely on behavioral and other indicators to detect fraudulent use of travel documents. For the inspection of the travel document itself, many officers at most ports we visited told us they generally rely on a few security features, such as watermarks and intaglio printing, and will look for signs of alteration; compare the photo and traveler; examine data on the biographic page, such as the expiration date; and examine the look and

---

feel of the document itself to determine whether the passport or visa is valid and is not fraudulently used by an imposter.

Primary officers also utilize a variety of tools and technology to assist in their inspection of security features in passports and visas. These include visual inspection tools, such as ultraviolet viewing equipment and handheld magnifying devices, to assist primary officers in identifying signs of alteration and counterfeiting that would not be detected otherwise. Primary officers can also query records of travelers by using the Treasury Enforcement Communications System (TECS)—an interagency database containing lookout information relating to the fraudulent use of travel documents, such as records of U.S. passports reported lost or stolen—or by using DHS’s U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) system to compare visa holders’ biometric records at entry with their records collected at issuance or prior entry.<sup>31</sup> US-VISIT is currently available at primary inspection at 116 air and 15 sea ports of entry, and in the secondary inspection areas at 154 land ports. Many primary officers who have visual inspection tools available told us they utilize these tools to check additional security features when their inspection of the two or three features they typically rely on was not satisfactory. In addition, officers who use the databases to inspect State-issued travel documents told us that access to information on visas issued by State has greatly improved their ability to reliably confirm the validity of visas and detect their fraudulent use.

---

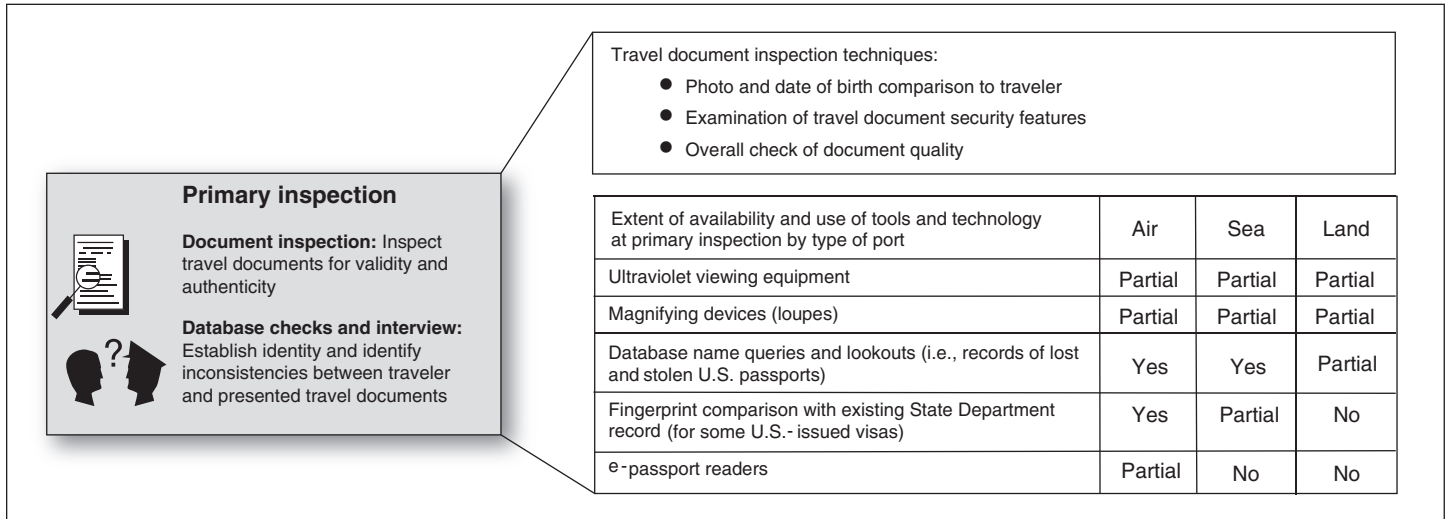
### Limited Availability and Use of Technology Limit Use of Security Features in Inspection of U.S. Passports and Visas

CPB officers at primary inspection are not fully able to exploit the security features in U.S. passports and visas due to the limited availability or use of tools and technology considered critical to ensuring the integrity of travel documents (see fig. 4). As a result, they do not always conduct checks against available records before admitting travelers to the United States. If the tools are not available, and the CBP officer determines additional scrutiny of travelers and documents are necessary, travelers will be referred to the secondary inspections area. At secondary inspections, CBP officers have more time and greater access to inspection-related technologies and equipment and, thus, are more capable of confirming the fraudulent use of U.S. passports and visas identified at primary inspection.

---

<sup>31</sup>To obtain a U.S. nonimmigrant visa, most foreign nationals are required to submit two fingerprint scans and a digital photo with their visa application. When visas are issued, applicants’ biographical data are shared with DHS’s US-VISIT, creating electronic records that can be checked against the data at the time of entry.

**Figure 4: Overview of the Process, Tools, and Technology for Primary Inspection of Travel Documents at U.S. Air, Sea, and Land Ports of Entry**



Source: GAO analysis of CBP data.

### Technology and Equipment to Assist Primary Inspection of U.S. Passports and Visas Are Not Fully Utilized

Though officers have various tools and technology available to them, the availability and use of equipment to conduct records and identity checks of travelers during primary inspection differ based on whether they arrive at air, sea, or land ports. In addition, these and other critical tools and technology are not consistently used at air, sea, and land ports of entry. For example, although CBP guidance states that visual inspection tools should be used and are extremely valuable for detecting counterfeit or altered passports and visas, CBP has provided tools to many, but not all, primary inspection workstations at air, sea, and land ports of entry. Moreover, use of these tools is a matter of port policy. At the air, sea, and land ports we visited, some officers told us they used these tools consistently, while other officers said they rarely used them.

Due in part to the large volume of travelers, primary officers at southern land ports only machine read—access a database that queries travelers’ records—travel documents or manually enter travelers’ biographic data to query records in TECS when deemed appropriate for the inspection situation, given the local traffic flow and traveler wait times. For example, at the southern land border ports we visited, CBP officers stated that currently only about 40 percent of travel documents that are machine readable are actually machine read during primary inspections, although this percentage has been rising in the last several years. CBP supervisor and inspection officers told us that officers are not restricted in their

---

inspection of travel documents and are able to machine read a document should they deem it necessary. In addition, CBP policy requires that all non-BCC visa holders be referred to secondary inspection at land ports of entry, according to CBP. In contrast, CBP told us that officers on the northern border are required to read all machine readable documents, and at air ports, officers consistently query travelers' records to identify lookout information on U.S. passports and visas.

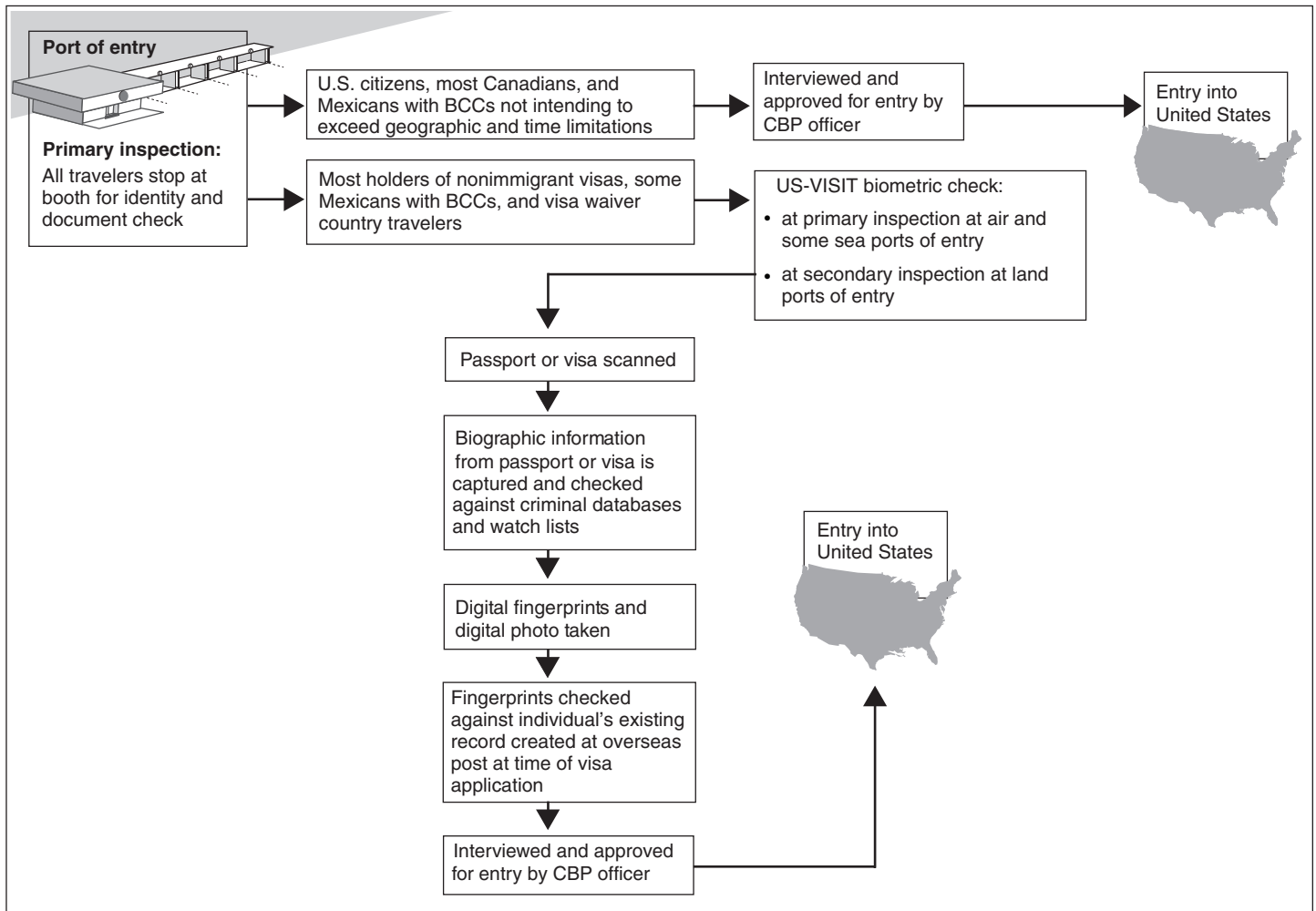
Most travelers presenting BCCs at southern land ports are generally not subject to US-VISIT requirements, although primary inspection officers can refer BCC holders to secondary inspection for US-VISIT screening.<sup>32</sup> However, only a small percentage of travelers with BCCs are referred for a US-VISIT screening (see fig. 5)—in particular, only if a primary officer determines travelers are traveling beyond their geographic limits or exceeding the number of travel days allowed, or if there are concerns about the traveler. Without the use of US-VISIT systems, officers observe and interview travelers and compare the photo and data in the BCC with the bearer of the document, but do not have the benefit of looking for discrepancies between the information provided by the travelers and the fingerprint data in the system. CBP officials stated there are no current plans to expand the use of biometric checks on travelers presenting BCCs due, in part, to concerns about extending the inspections processing time at primary inspection and space constraints at land ports. However, CBP acknowledges the use of biometric checks of travelers presenting BCCs, when available, provides additional verification that travel documents are valid and belong to travelers presenting the documents, helping to address imposter fraud—the most significant type of fraud associated with BCCs. CBP officers intercepted nearly 16,000 BCCs used by imposters in fiscal year 2006.

---

<sup>32</sup>BCCs can be machine-read at primary inspection in southern land ports, displaying the biographic data for the CBP officer to compare to the presented document.



**Figure 5: Overview of US-VISIT Procedures at Air, Sea, and Land Ports of Entry**



Sources: GAO (analysis); MapArt (map).

In addition, DHS is not fully exploiting at primary inspection a key security feature of the new U.S. e-passport—the chip. Specifically, because DHS has not fully deployed e-passport readers at all primary inspection areas, officers cannot routinely read and authenticate the chip in e-passports, which would better enable officers to detect many forms of passport

---

fraud, including photo substitution and imposters.<sup>33</sup> Without an e-passport reader, inspection officers do not have the benefit of comparing the traveler with the photograph and biographic information stored in the RFID chip of the e-passport. DHS deployed, in response to a legislative requirement, a total of 212 of these readers for use on foreign e-passports at 33 out of 116 air ports of entry. These 33 air ports were chosen because they process the largest volume of travelers—about 97 percent—from Visa Waiver Program countries.<sup>34</sup> The remaining readers are used for training purposes. While the same e-passport readers may also be used to read the chip in U.S. e-passports, U.S. citizens are primarily processed through specific lanes at these air ports that are not equipped with e-passport readers.

CBP has no schedule to install e-passport readers to primary inspection lanes for U.S. citizens at air ports or to install e-passport readers at sea and land ports of entry. CBP has also not defined the specific conditions that should be in place to expand the deployment of e-passport readers to additional ports. CBP officials indicated they intend to install e-passport readers at additional ports in the future. These officials noted several factors for why they have not installed additional readers or developed a planned schedule to do so, including the need for additional funding and advancements in the software technology for the readers. CBP officials stated that further funding would have to be allocated to expand the deployment of e-passport readers at air, land, and sea ports of entry and that a request has been made to DHS to include additional funding in the

---

<sup>33</sup>CBP officers use e-passport readers to access the biographic information and digitized photo stored on the RFID chip of e-passports. To read e-passports, officers place the biographical page of the e-passport on the reader's glass plate. The reader then electronically scans the biographical information—including the document type, issuing country code, document number and bearer name, bearer nationality, date of birth, gender, and document expiration date—to access the biographical data and digital photograph embedded in the e-passport's RFID chip. Once the biographical data and photograph are displayed on the primary inspection computer screen, the officer compares the information displayed with the passport photo and information on the biographic page and verifies the data extracted from the RFID chip are valid and not fraudulent.

<sup>34</sup>The Enhanced Border Security and Visa Entry Reform Act of 2002 requires, for Visa Waiver Program countries, that passports be machine readable, tamper resistant, and incorporate biometrics and document authentication identifiers and that DHS deploy equipment and software necessary to biometrically compare and authenticate these documents. DHS has interpreted this provision to require applicants for admission under Visa Waiver Program who are traveling on a passport issued on or after Oct. 26, 2006 to present an e-passport, and DHS deployment and use of e-passport readers as of that same date, according to DHS.

---

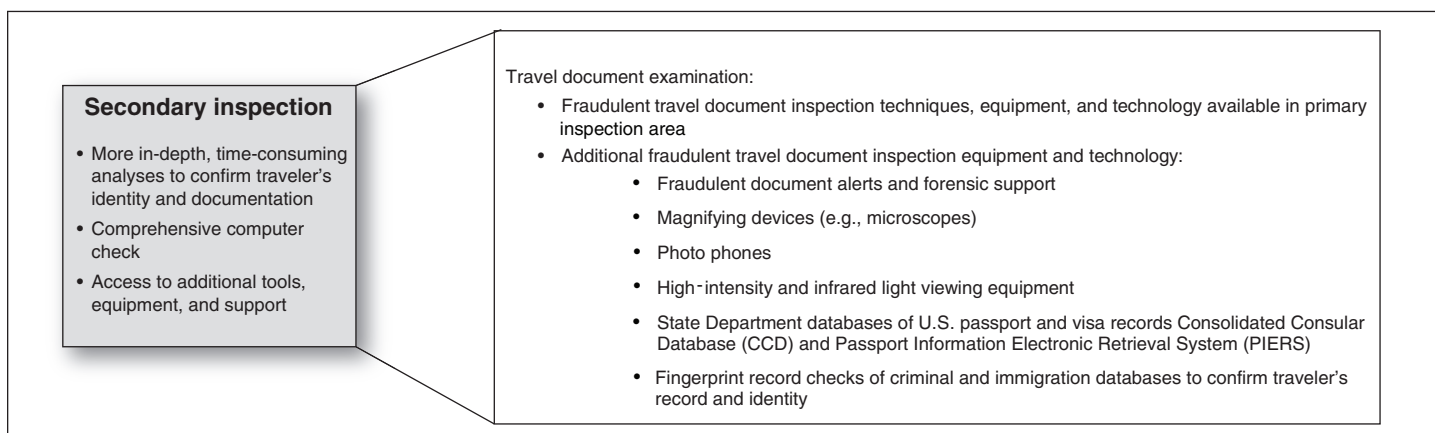
agency's fiscal year 2009 budget. As of June 2007, CBP has been unable to provide additional information on the details of this budget request. CBP officials also said that due to the current software, the new e-passport readers are slower than current inspection machines and could possibly extend the inspection-processing time for U.S. citizens—negatively affecting land ports already experiencing extensive wait times for inspections.

In addition, the e-passport reader software is currently not programmed to validate e-passports' digital signatures, which ensure the data stored on the RFID chip are authored by an issuing authority—the State Department in the case of U.S. e-passports—and have not been altered. Although DHS officials stated the current reading of the chip in foreign and U.S. e-passports does not fully verify the digital signatures, State and DHS are drafting a memorandum of understanding to govern interagency use of a validation service—DHS's e-passport Validation Service and Repository—to verify the integrity and validity of electronically stored data on e-passports received at ports of entry.

Equipment and Technology Available at Secondary Inspections to Confirm the Fraudulent Use of U.S. Passports and Visas

Once a CBP officer at primary inspection intercepts passports or visas that are suspected of being fraudulently used or counterfeit, secondary inspection officers have more time to question travelers, review the validity and authenticity of travel documents, and conduct database checks to confirm the travelers' identities. In addition, officers conducting secondary inspection are more experienced and trained to use support not available at primary inspection, such as tools and equipment for forensic examination of suspected fraudulent U.S. passports and visas, and additional forensic support and intelligence information from outside sources, such as DHS's Forensic Document Laboratory (FDL) (see fig. 6).

**Figure 6: Overview of the Process, Tools, and Technology for Secondary Inspection of Travel Documents at U.S. Ports of Entry**



Source: GAO analysis of CBP data.

Officers at secondary inspection have access to more tools and equipment and more time with which to examine the security features of suspected fraudulent travel documents than do officers at primary inspection. For example, secondary inspection areas generally have a variety of magnifying devices and microscopes to detect data alterations, photo and page substitutions in passports, and altered or counterfeit visas. In addition, secondary officers generally have access to high-intensity light devices, which allow for the inspection of certain paper disturbances often caused by erasures, for example. Recently, some ports have received a laboratory workstation that secondary officers can use to examine questionable travel documents under different types of lighting and at various magnifications.

CBP officers in secondary inspection also have access to additional databases to confirm travelers' identities and verify the authenticity of U.S. passports and visas. For example, secondary officers have access to databases containing lookout information and travelers' biometric data, including photographs and fingerprints. In addition, secondary officers have access to State's databases to confirm data on nonimmigrant visa and passport issuance; State's Consular Consolidated Database (CCD), which stores information about visa applications, issuances, and refusals; and State's Passport Information Electronic Retrieval System (PIERS), which provides similar data on passport issuance to confirm the identity and authenticity of U.S. passports.

---

During secondary inspections, officers can seek support outside the port to assist in confirming travel document fraud. For example, DHS's FDL provides forensic document analysis and law enforcement support services to secondary officers in real time, 7 days a week. Some ports are equipped with photophones to transmit images of documents to FDL experts for verification of altered and counterfeit U.S. passports and visas, and secondary officers can forward suspected fraudulent U.S. passports and visas to FDL experts for a thorough forensic examination. In addition, to inform officers of fraudulent trends concerning travel documents, secondary inspection areas maintain archived intelligence information from a number of sources, including FDL, State, and intelligence officers at the port, that details how U.S. passports and visas have been fraudulently used in the past. Although CBP officers are responsible for reviewing alerts on the fraudulent use of U.S. passports and visas they receive by e-mail and daily briefings, secondary inspection areas maintain hard copies of intelligence information on file for officers to review, as needed. In addition, archived alerts are also available through electronic databases, such as the DHS's intranet, which officers can choose to access in the secondary inspection area.

---

### Officers Lack Sufficient Training on the Security Features and Fraudulent Trends of U.S. Passports and Visas

CBP did not update its training program for all officers to include information on the security features in the e-passport before State began issuing this travel document. Between the summer of 2006 and March 2007, State provided exemplars—genuine documents for training purposes—of the e-passport to a variety of entities, including its U.S. missions overseas, foreign governments, FDL, and DHS, according to State documentation. We found that CBP was not provided with exemplars prior to issuance of the new e-passport. Although State began issuing e-passports as early as December 2005, CBP was not provided with e-passport exemplars until March 2007, according to State documentation. According to CBP officials, training on the features of the new e-passport was not provided to officers at basic training until April 2007. In addition, CBP has not provided formal training utilizing e-passport exemplars to officers at all ports of entry, although training with e-passport exemplars was provided to officers at the 33 airports where e-passport readers were installed, according to CBP officials.

State officials explained that preparing exemplars is a time-consuming process and that meeting production demands limited the supply of document exemplars. Therefore, according to State, exemplars were provided only to FDL and foreign embassies located in Washington, D.C., prior to the issuance of the e-passport. To provide information on the

---

features of the new documents, FDL prepared an alert for CBP and other law enforcement entities outlining the details of the security features in the e-passport and new emergency passport. Without an official exemplar, a CBP training officer at one port we visited used his own e-passport to provide officers training on the security features of the e-passport. This training officer stated that while he used the FDL alert to train officers, use of the alert alone does not provide officers with an understanding of the look and feel of the actual document. In addition, CBP officers at several ports we visited stated they had inspected e-passports but were not aware of how the security features of the e-passport differed from previous generations and how changes to the security features addressed the types of fraudulent attacks commonly committed against older generations of passports.

Lack of Ongoing Training  
Impedes Officers'  
Understanding of Security  
Features of Valid Generations  
of Passports and Visas at Some  
Ports

Given evolving fraud trends and the quality of attempts to alter passports and visas, ensuring officers are properly trained to recognize the fraudulent use of these travel documents is essential. Training officers at most of the ports we visited identified the importance of continual training on the security features and evolving fraudulent trends related to all generations of valid passports and visas; however, the extent to which mandatory training is supplemented by refresher training in the subject varied among these ports. For example, two ports we visited provide continual training on fraudulent document detection to all officers yearly, while other ports provided refresher training less frequently. While CBP requires officers to complete courses that include segments in fraudulent document detection relating to passports and visas, CBP officials stated there is currently no program in place to ensure officers receive such training continually. Some senior officers at some of the ports we visited stated they had not been retrained on the security features of passports and visas and fraudulent document detection since basic training.

CBP officials explained that the need to balance officers' inspections responsibilities with training limits training opportunities. At most of the ports we visited, port officials explained there is not enough time to provide all officers with additional training on the security features of valid generations of passports and visas due to inspection priorities and limited staffing at ports. To provide greater opportunities for continual document examination training relating to passports and visas, many ports we visited undertook their own training initiatives. For example, four of the ports added segments on fraudulent document detection to mandated courses that did not already include such information. In addition, based on training developed in the field, CBP developed a Web-based course on the security features of visas. Officials at ports undertaking these

---

initiatives said they realized that without continual training, officers often felt less prepared to understand and recognize security features and fraudulent trends. They stated that because passports and visas could remain valid for 10 years, fraudulent attacks committed against older generations of these travel documents often recur, and officers should be reminded of these fraud trends through continuing training. In addition, to identify and adopt best practices on fraudulent document detection training, CBP held a forum in January 2005 that led to the development of a nationwide training effort requiring supplemental training on fraudulent document detection at all ports. However, CBP does not have any plans to hold such forums in the near future, and while CBP encourages ports to adopt initiatives to improve the delivery of refresher training on the examination of passports and visas, it is often not possible to mandate initiatives that are appropriate for all ports because ports differ in the types of fraudulent travel documents they encounter.

---

## Conclusions

Ensuring the integrity of passports and visas is an essential part of border security requiring continual vigilance and new initiatives to stay ahead of those seeking to enter the United States illegally. Preventing the fraudulent use of travel documents requires a combination of enhanced document features, solid issuance measures, and an inspection process that utilizes the security features of these documents. A well-designed document has limited utility if it is not well-produced or the inspection does not utilize the available security features to detect attempts to falsely enter the United States. State has added technical features and security techniques to the design and production of these documents that make it much harder to counterfeit or alter new generations of passports and visas. Nonetheless, older documents have been fraudulently used. Further, counterfeit and alteration threats to the security of these documents are always changing, requiring regular reassessments of the security features in the documents' design. In addition, because it takes several years to address a vulnerability that has been identified in a document's design, a structured process for reassessing the features and planning for new generations of these documents is critical. State has also strengthened the issuance process for visas and passports. Despite some improvements, however, the passport issuance process remains vulnerable, especially at the application acceptance stage, where oversight of the thousands of acceptance facilities—responsible for verifying the identity of applicants—remains weak. Finally, many CBP inspectors at U.S. ports of entry face time constraints in processing large volumes of people and therefore rely on a few visual and tactile security features of passports and visas, in addition to their interviews, to identify fraudulent use of these documents.

---

Moreover, CBP officers are unable to take full advantage of the improved technical and security features in passports and visas because of insufficient training and uneven access to equipment. While it would not be possible to remove all risks inherent in issuing and inspecting travel documents, or to foresee all evolving counterfeit and alteration threats, we believe that more systematic testing, planning, oversight, and data analysis practices could enhance border security.

---

## Recommendations for Executive Action

We are recommending that the Secretary of State take the following two actions to improve the integrity of its travel documents.

- Develop a process and schedule for periodically reassessing the security features and planning the redesign of its travel documents.
- Establish a comprehensive oversight program of passport acceptance facilities. In doing so, State should consider conducting performance audits of acceptance facilities, agents, and accepted applications and establishing an appropriate system of internal controls over the acceptance facilities.

We are also recommending that the Secretary of Homeland Security take the following two actions to more fully utilize the security features of passports and visas.

- Develop a deployment schedule for providing sufficient e-passport readers to U.S. ports of entry, which would enable inspection officials to better utilize the security features in the new U.S. e-passport.
- Develop a strategy for better utilizing the biometric features of BCCs in the inspection process to reduce the risk of imposter fraud.

Finally, we are recommending that the Secretaries of State and Homeland Security collaborate to provide CBP inspection officers with better training for the inspection of travel documents issued by the State department, to better utilize the security features. This training should include training materials that reflect changes to State-issued travel documents in advance of State's issuance of these documents, including the provision of exemplars of new versions of these documents in advance of issuance.



---

## Agency Comments and Our Evaluation

We provided draft copies of this report to the Secretaries of State and Homeland Security and to the U.S. Public Printer at the Government Printing Office for review and comment. We also provided a draft copy to the Department of Commerce's National Institute of Standards and Technology. We received written comments from State and DHS, which are reprinted in appendixes VI and VII, respectively. State, DHS, GPO and NIST provided technical comments which we have incorporated in the report, as appropriate. State and DHS concurred with the findings and recommendations of the report.

State agreed with our recommendations and described the actions it is taking and plans to take to implement them. State also provided additional information on the Consular Consolidated Database (CCD), recent visa fraud cases, and the ways in which State identifies fraudulent passports and visas.

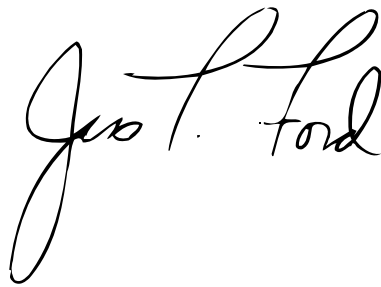
DHS concurred with our recommendations and described the actions it is taking and plans to take to implement them. DHS believes it has already implemented our recommendation that it develop a strategy for better utilizing the biometric features of BCCs in the inspection process. We agree that DHS's US-VISIT capability enables primary inspectors at air and some sea ports of entry to use fingerprint biometrics to compare and authenticate the document and holder of visas and BCCs. However, at land border ports this capability is not available in primary inspection. Furthermore, travelers with BCCs at southern land border ports—the ports where BCC imposter fraud is most significant—are not routinely referred to secondary inspection, where they do have the capability to utilize the fingerprint records for comparison, and all BCCs are not machine-read for access to the biographic data during inspection at these ports of entry. As a result, inspectors are not making full use of the biometric information available for BCCs. To more fully utilize the available fingerprint biometric in the BCC and mitigate imposter fraud, we are suggesting that DHS develop a strategy to better use both fingerprint biometric of the BCC and increase card reads of the BCC in primary inspection at southern land border ports of entry.

---

We are sending copies of this report to the Secretaries of State and Homeland Security, the U.S. Public Printer at the Government Printing Office, as well as the Director of the National Institute of Standards and Technology. We will also make copies available to others on request. In addition, the report will be available at no charge on the GAO Web site at <http://www.gao.gov>.

---

If you or your staff have any questions about this report, please contact me at (202) 512-4268 or [fordj@gao.gov](mailto:fordj@gao.gov). Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made contributions to this report are listed in appendix VIII.

A handwritten signature in black ink that reads "Jess T. Ford". The signature is written in a cursive style with a large, looping initial "J" and a distinct "T" and "F".

Jess T. Ford  
Director, International Affairs and Trade

---

# Appendix I: Scope and Methodology

---

To examine the features in passports and visas, we reviewed relevant documentation, including materials on the security features, available counterfeit deterrence and durability studies, fraud bulletins and alerts, and regulations. We also interviewed officials at Department of State's Consular Affairs Bureau, Department of Homeland Security's (DHS) Forensic Document Laboratory (FDL), the Department of Commerce's National Institute of Standards and Technology (NIST), and the Government Printing Office (GPO). To identify required and recommended standards for international travel documents, we reviewed documentation from the International Civil Aviation Organization and attended the organization's machine-readable travel document symposium in Montreal, Canada. To identify the process for addressing potential risks, we reviewed documentation and interviewed officials at State's Consular Affairs Bureau, FDL, and NIST. To identify how State obtains, analyzes, and shares information on the features and fraudulent use of these documents, we reviewed relevant documentation, including fraud bulletins and alerts, and met with State officials from the Diplomatic Security and Consular Affairs Bureaus, including the fraud prevention units of passport and visa services, as well as with DHS officials from CBP and FDL.

To examine the integrity of the issuance process for these documents, we reviewed relevant documentation, including reports and audits of internal controls and production and issuance procedures, and interviewed officials at State's Consular Affairs Bureau. We also conducted site visits and interviewed officials at seven domestic passport offices and two U.S. consulates in Mexico. To examine how passport fraud is committed during the issuance process, we reviewed State Department Bureau of Diplomatic Security and Bureau of Consular Affairs statistics on passport fraud. We also met with officials at State's Diplomatic Security Headquarters Criminal Division and at Diplomatic Security's Field Offices in Los Angeles, Seattle, Miami, Chicago, Boston, and Portsmouth, New Hampshire. We visited State's passport-issuing offices in Los Angeles, Seattle, Miami, Chicago, Boston, Portsmouth, and Washington, D.C. We chose the Portsmouth office because it is one of the two passport "megacenters" responsible for adjudicating applications from other regions. We chose these locations to gain an appropriate mix of geographic coverage, workload, and levels and types of passport fraud. We did not select these locations to be generalizable to all passport offices, but rather to obtain an appropriate mix of geographic coverage and workload. We analyzed fraud referral statistics from State's office of passport services and Diplomatic Security for fiscal years 2002 through 2006. Together with passport services officials, we identified the methods used to capture and compile the data and determined that the data were

sufficiently reliable and generally usable for the purposes of our study. At five of the seven offices we visited, we conducted interviews with various officials and interviewed passport examiners chosen by office management, although we provided input into the selection of examiners and interviewed these individuals without the presence of management. We also met with Diplomatic Security agents attached to field offices responsible for investigating fraud suspected at the offices we visited. In addition, we interviewed relevant State officials at Passport Services, Diplomatic Security, and the Office of the Inspector General.

To examine the measures taken to ensure the integrity of blank passports, we visited the GPO production facilities in Washington, D.C., and observed the production of blank passports; interviewed relevant GPO and GPO Inspector General officials about the measure taken throughout the production and delivery processes; and reviewed GPO Inspector General reports on audits of the security aspects of blank passport production and transportation. To examine the measures that have been taken to strengthen the issuance process for visas, we reviewed past GAO reports and interviewed State officials in the Visa Office. To identify the measures taken to ensure the integrity of blank visa foils prior to delivery to State custody, we interviewed GPO officials and reviewed relevant GPO documents. To examine the measures taken to ensure the integrity of the border crossing card (BCC), we visited two production facilities in Vermont and Nebraska where BCCs are produced. We interviewed production and management staff at both of these facilities. We identified and reviewed past GAO and Inspector General reports on the internal controls and audits in place for the visas process. For BCCs, we identified the internal controls and measures that differ from the normal visa process, but did not assess compliance with these controls.

To examine the inspection measures and processes for travel documents issued by the State Department at U.S. ports of entry, we reviewed relevant documentation and interviewed officials at DHS's U.S. Customs and Border Protection (CBP), FDL, and U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) program, and conducted site visits to ports of entry. We reviewed CBP inspections program policies, procedures, and related memorandums and relevant laws and regulations. At headquarters, we met with CBP officials responsible for field operations, information technology, training and development, intelligence, and information technology. We also interviewed officials from the Federal Law Enforcement Training Center and FDL about issues relating to document examination training, and we discussed with FDL officials the types of forensic document analysis and operational support

services provided to CBP. In addition, we interviewed US-VISIT officials and reviewed relevant documentation on the deployment and use of inspections-related technologies.

To observe inspections processes and measures, we conducted site visits to nine U.S. ports of entry. Due to differences in travel document inspections processes and measures among air, sea, and land ports, we selected three ports of each type. Air ports of entry included Chicago O'Hare, Dallas/Fort Worth, and Miami. Sea ports of entry included Los Angeles/Long Beach, Miami, and Port Everglades, Florida. Land ports of entry included Laredo, Texas; Limestone/Houlton, Maine; and San Ysidro, California. We selected a nongeneralizable sample of air, sea, and land ports that ensured we included a range of the characteristics that can cause variation in the inspections process. Using CBP inspections program performance data, we selected ports that had high and medium levels of fraudulent documents, based on the total and average number of fraudulent travel documents intercepted, and the ratio of total travelers inspected to total fraudulent documents intercepted for fiscal years 2000 through 2005. We also selected ports based on a geographic mix, to include land ports on the Mexican and Canadian border, and a mix of ports in the northern, eastern, southern, and western regions of the United States. At each of these ports we met with port directors, CBP officers responsible for intelligence information and training, observed CBP officers conducting primary inspections, and reviewed procedures and the equipment available in primary and secondary inspection areas to examine State Department-issued travel documents. At some ports, no travelers were referred for secondary inspections for the fraudulent use of State Department-issued travel documents at the time we observed inspections; however, CBP officers provided us with an overview of secondary inspection procedures and resources. In addition to the nine ports of entry we selected, we conducted preliminary site visits to the Nogales, Arizona, land port of entry, and the Los Angeles and Washington Dulles air ports of entry. During these preliminary site visits, we observed primary and secondary inspection processes and equipment and interviewed CBP officials.

We conducted our work from June 2006 through May 2007 in accordance with generally accepted government auditing standards.

---

# Appendix II: Types of Passports

---

State issues four types of passports: tourist, official, diplomatic, and emergency.

- A tourist passport, for individuals 16 years or older, is valid for 10 years from the date of issuance; it is valid for 5 years for younger applicants.
- An official passport, for federal employees traveling on official government business, is valid for 5 years from the date of issuance.
- A diplomatic passport, for government officials with diplomatic status, is valid for 5 years from the date of issuance.
- An emergency passport, for individuals overseas who no longer possess a valid passport, may be valid for up to 1 year or, in cases of repatriations, limited to direct return to the United States.

In conjunction with the rollout of the new e-passport, State also began issuing a new emergency passport in August 2006, representing the first time that U.S. embassies and consulates issued a standard-design emergency passport. Prior to the emergency passport, U.S. embassies and consulates used the 1994 or earlier versions to issue a passport for emergency purposes. The emergency passport resembles the e-passport except that it is personalized using a foil that is stuck in the book in a manner similar to a visa foil.

The passport card is expected to be valid for 10 years from the date of issuance for individuals 16 years or older and valid for 5 years for younger applicants. State plans to issue the passport card in 2008.

---

# Appendix III: Testing Conducted in Development of E-Passport Design

---

To test the passport design, State requested expertise from FDL and NIST. Specifically, FDL conducted counterfeit deterrence studies on the security features of the diplomatic and tourist e-passport in 2005. FDL had conducted similar studies for State in the past on the 1998 tourist passport. In addition, State asked FDL to test the physical security of the e-passport using the diplomatic e-passport. Results of FDL tests were incorporated into the design prior to the issuance of the tourist passport. NIST also conducted tests, such as durability testing, to evaluate the technical merits of passport books and to inform GPO and State's decisions for awarding contracts to suppliers. While there is a provision in the awarded contracts to conduct long-term durability testing, NIST has not been asked to provide these tests. In addition, in response to security and privacy concerns, NIST was requested to evaluate the vulnerability of the e-passport chip to remote access by an unauthorized party.

Additional tests were also conducted at airports to assess the performance of the new e-passport in an actual inspection environment. For example, tests were conducted with airlines in which holders of U.S. diplomatic and official e-passports presented their e-passports for inspection when arriving in the United States at select airports. These tests were conducted to gather information on the accuracy and speed in reading the chip to support the development and implementation of the e-passport. State incorporated the results from the tests to improve the design.

---

# Appendix IV: Issuance Process for Passports and Visas

---

## Passport Issuance Process

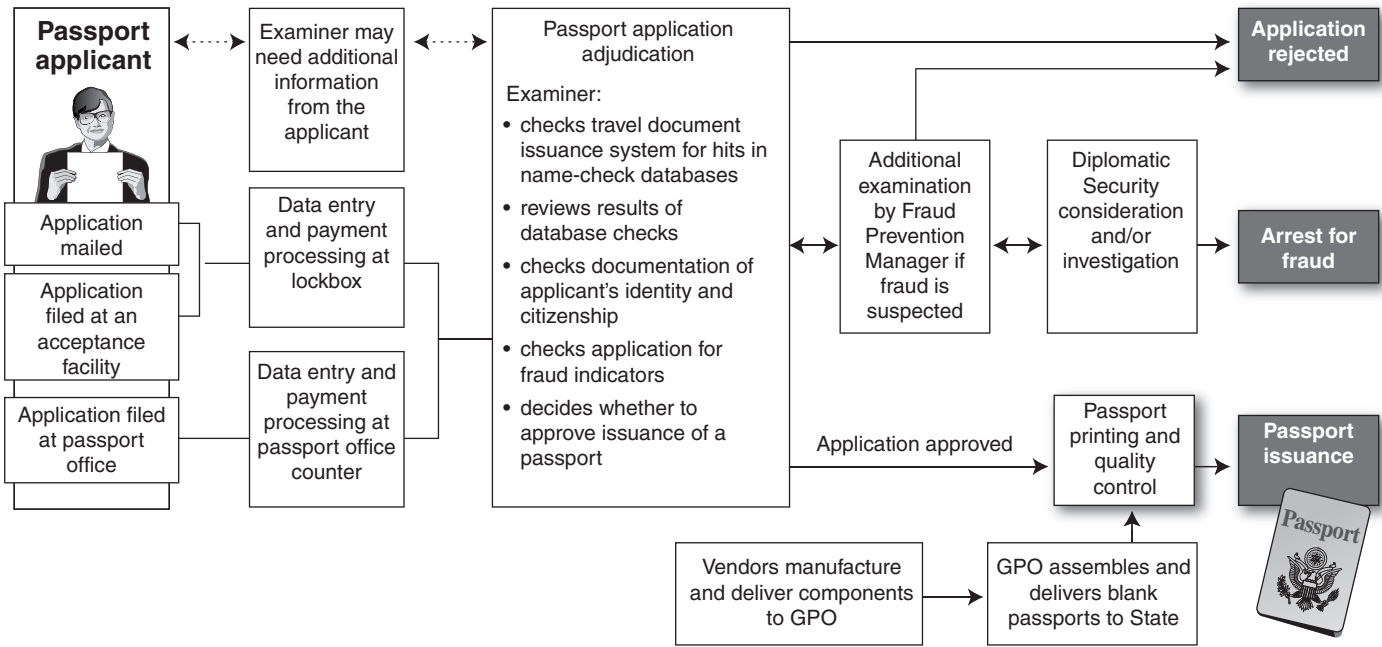
Once a passport application has been received by one of the 17 domestic passport-issuing offices, each application must be examined by a passport examiner who determines, through a process called adjudication, whether the applicant should be issued a passport. Adjudication requires the examiner to scrutinize identification and citizenship documents presented by applicants to verify their identity and U.S. citizenship.<sup>1</sup> When examiners detect potentially fraudulent passport applications, they refer the applications to their local fraud prevention program for review, with potential referral to State's Bureau of Diplomatic Security for further investigation. Once an applicant has been determined eligible for a passport by a passport examiner, the passport is personalized with the applicant's information at one of the domestic passport-issuing offices or the production facility and then delivered to the applicant. For an overview of the passport process, see figure 7.

---

<sup>1</sup>The passport adjudication process is facilitated by computer systems, which automatically check the applicant's name against several databases. In addition, examiners scrutinize paper documents and other relevant information, watch for suspicious behavior and travel plans, and request additional identification when they feel the documents presented are insufficient.



Figure 7: Application and Issuance Process for Passports



Sources: GAO analysis of State Department data; Nova Development (clip art).

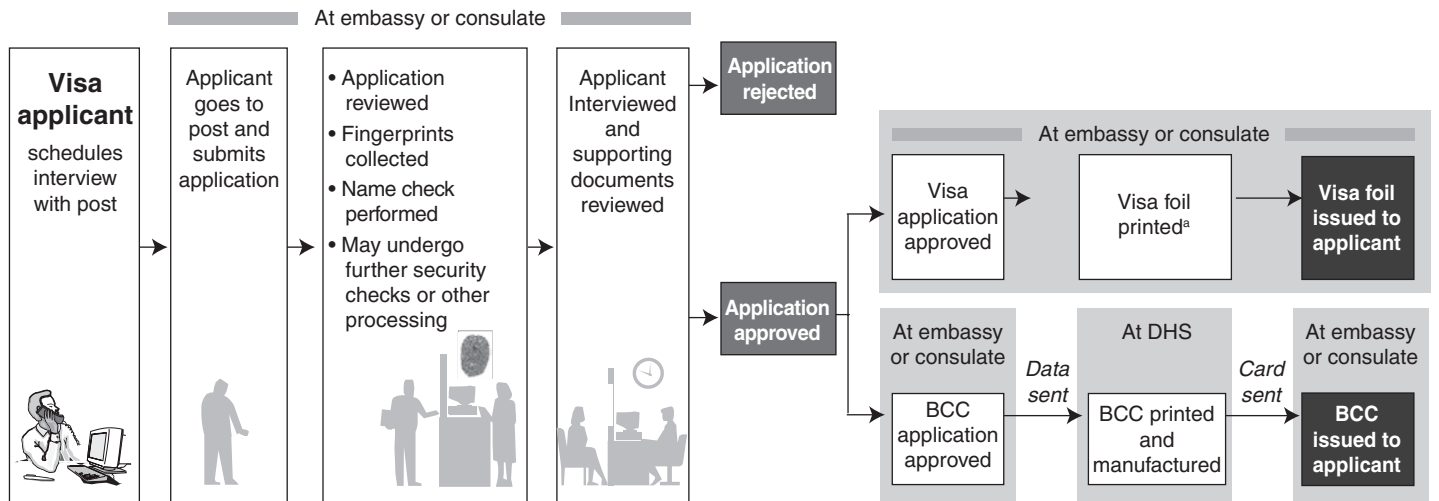
## Visa Issuance Process

DHS is responsible for establishing visa policy, reviewing implementation of the policy, providing additional direction, and reviewing petitions for immigration. State manages the visa process, as well as the consular corps and its functions at 219 visa-issuing posts overseas, and provides guidance, in consultation with DHS, to consular officers regarding visa policies and procedures.<sup>2</sup> GPO overseas the production of blank visa foils. Visas foils are personalized at posts overseas with the applicant's personal

<sup>2</sup>The 1952 Immigration and Nationality Act, as amended, is the primary body of law governing immigration and visa operations (P.L. 82-414, 8 U.S.C. § 1101 et seq.). The Homeland Security Act of 2002 (P.L. 107-296) generally grants DHS exclusive authority to issue regulations on, administer, and enforce the Immigration and Nationality Act and all other immigration and nationality laws relating to the functions of U.S. consular officers in connection with the granting or denial of visas. State retains authority in certain circumstances as outlined in the act. A September 2003 memorandum of understanding between State and DHS further outlines the responsibilities of each agency with respect to visa issuance.

information, attached to the foreign passport, and delivered to the applicant. DHS's U.S. Citizenship and Immigration Services produces and personalizes BCCs once an applicant has been determined eligible by a consular officer and delivers the cards to State for distribution by the U.S. mission in Mexico. For an overview of the visa process, see figure 8.

Figure 8: Application and Issuance Process for Visas



Sources: GAO analysis of State Department data; Nova Development (clip art).

\*Visa foils are manufactured by contractor under supervision of GPO and State.

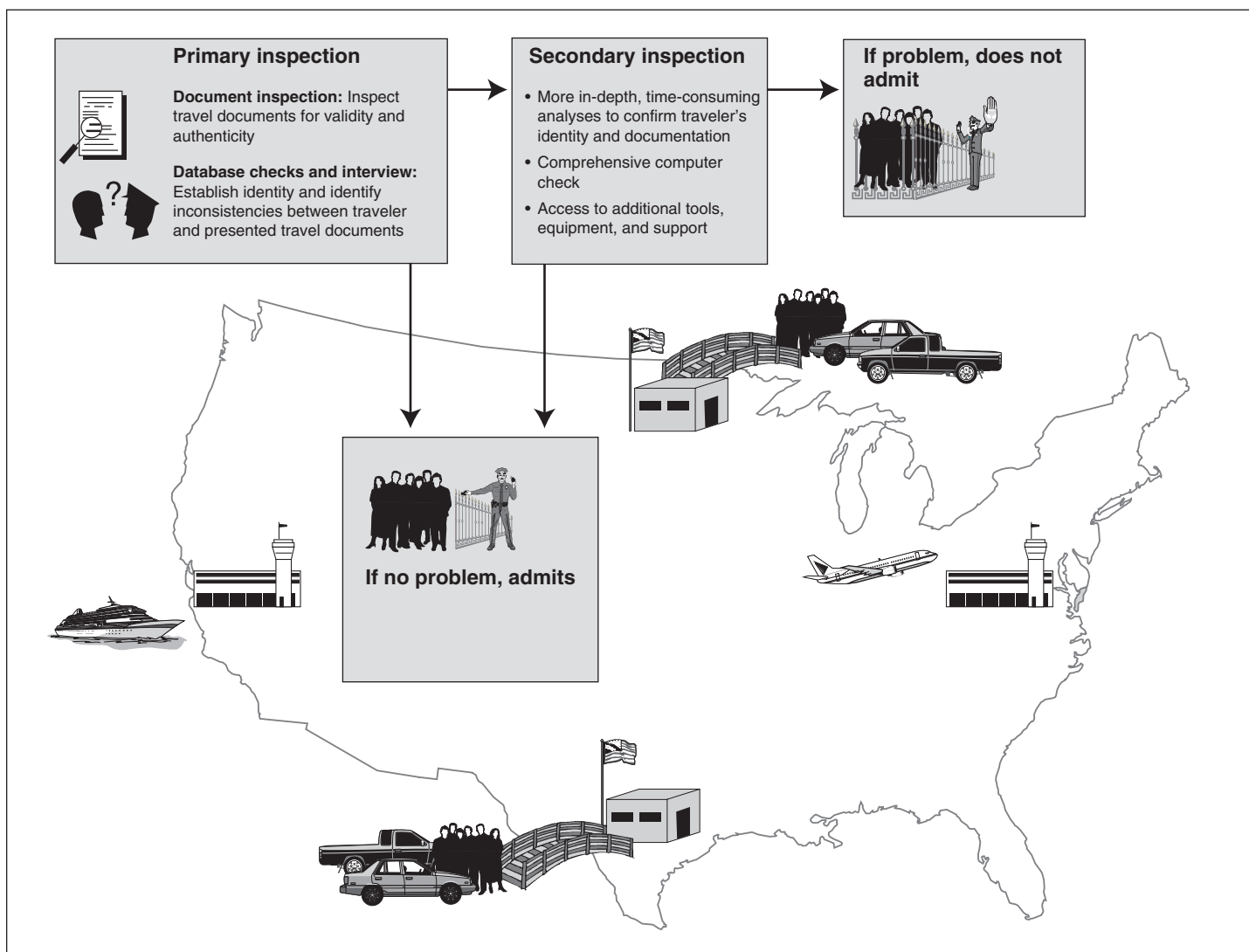
---

# Appendix V: Primary Inspection Processes at Air, Sea, and Land Ports of Entry

---

The primary inspection process for passports and visas varies at air, sea, and land ports of entry due to differences in ports' environments and the risk each type of port faces with regard to fraudulent travel documents. In addition, the mode of travel and how travelers bearing passports and visas enter dictate the primary inspection procedures. For example, while at each port, primary officers question travelers regarding their identity and purpose of travel, and examine their passports or visas, the availability and use of equipment to conduct identity and records checks of travelers during primary inspection differ based on whether travelers arrive by plane, sea vessel, vehicle, or on foot. If the primary officer determines that further review is needed, the officer will refer the traveler to secondary inspection. In secondary inspection, an officer makes a final determination to admit the traveler or deny admission for reasons such as the presentation of a fraudulent or counterfeit passport or visa. Once a CBP officer in secondary inspection has determined a document is fraudulent or is being presented by a traveler other than the rightful holder, the officer processes the traveler as inadmissible and ensures that information about the document is distributed promptly. Information about seized fraudulent and counterfeit passports and visas is regarded as possible intelligence that may have a connection to other criminal activities and national security concerns, such as terrorism. See figure 9 for an overview of the inspection process at U.S. ports of entry.

Figure 9: Inspection Process for Entry into the United States



Sources: GAO analysis of Immigration and Naturalization Service data; Nova Development (clip art).

- Air Ports of Entry:* Prior to travelers' arrival, for flights to the United States, commercial airlines are required to submit passenger and crew manifests containing first and last names, dates of birth, nationalities and passport numbers to CBP through the Advanced Passenger Information System (APIS). With information from APIS, CBP officers conduct queries of lookout records for each traveler in the Treasury Enforcement Communications System (TECS). TECS queries provide officers with

lookout information on travelers, including alerts of lost and stolen travel documents that may be used fraudulently. In addition, primary officers query records of U.S. visas to verify the State Department's visa information. For a traveler with a U.S. nonimmigrant visa subject to processing in DHS's U.S. Visitor and Immigrant Status Indicator Technology (US-VISIT) systems, primary officers collect scans of the traveler's two fingerprints (the right and left index fingers) and take a digital photograph of the traveler. The computer system compares the two fingerprints against existing records collected at issuance to confirm that the traveler is the person to whom State issued the U.S. visa.

- *Sea Ports of Entry:* At sea ports of entry, commercial carriers are required to submit passenger manifests to CBP through APIS prior to docking, and CBP officers analyze TECS data using APIS to identify passengers requiring further examination when they enter the United States. Some seaports have automated terminals with computer systems equipped with TECS and US-VISIT systems, and the inspections process is similar to that of an air port. Other sea ports have nonautomated terminals that are not equipped with computer systems. At these terminals, primary inspections occur onboard or dockside, where officers rely on the advanced TECS checks and do not conduct US-VISIT biometric checks. Officers at the sea ports we visited stated the risk of travelers presenting fraudulent travel documents at seaports is not as significant as at air and land ports of entry, as most cruise ship passengers begin and end their trips in the United States, and crew members often make several entries and are inspected each time.

*Land Ports of Entry:* CBP has established procedures to inspect travelers expeditiously at land ports due to the large volume of travelers arriving on foot and in vehicles at land ports of entry—more than 85 percent of all entries into the United States. Primary officers perform pedestrian and vehicle inspections usually with no advanced passenger information and do not consistently conduct record checks in TECS. In addition, primary inspection procedures differ for pedestrians and vehicles. For pedestrians, if TECS is available, the traveler's name can be machine read from the travel document or manually keyed in by the primary officer. For vehicles, officers frequently inspect multiple travelers entering in a single vehicle, and the TECS queries are conducted primarily on the vehicle data to refer the vehicle and travelers for secondary inspection. Documents and names of the vehicles' occupants are generally checked randomly or when the officer suspects something is wrong. In addition, travelers with nonimmigrant visas or border crossing cards requiring additional US-VISIT processing are sent to secondary inspections areas. In general, at land ports, officers rely on visual observation, interviewing skills, and a quick

---

**Appendix V: Primary Inspection  
Processes at Air, Sea, and Land  
Ports of Entry**

---

check of document security features and facial identification to identify imposters and determine secondary referrals.

# Appendix VI: Comments from the Department of State

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



**United States Department of State**

*Assistant Secretary for Resource Management  
and Chief Financial Officer*

*Washington, D.C. 20520*

**JUL 24 2007**

Ms. Jacquelyn Williams-Bridgers  
Managing Director  
International Affairs and Trade  
Government Accountability Office  
441 G Street, N.W.  
Washington, D.C. 20548-0001

Dear Ms. Williams-Bridgers:

We appreciate the opportunity to review your draft report, "BORDER SECURITY: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use," GAO Job Code 320440.

The enclosed Department of State comments are provided for incorporation with this letter as an appendix to the final report.

If you have any questions concerning this response, please contact Phil Linderman, Team Leader, Bureau of Consular Affairs, Office of Fraud Prevention Programs at (202) 647-0732.

Sincerely,

A handwritten signature in black ink, appearing to read "Bradford R. Higgins".

Bradford R. Higgins

cc: GAO – Monica Brym  
CA – Maura Harty  
State/OIG – Mark Duda

**Department of State Comments on GAO Draft Report**  
**Border Security: Security of New Passports and Visas Enhanced but More**  
**Needs to Be Done to Prevent Their Fraudulent Use**  
**(GAO Code 320440, GAO 07-1006SU)**

Thank you for the opportunity to comment on your draft report entitled *BORDER SECURITY: Security of New Passports and Visas Enhanced but More Needs to Be done to Prevent Their Fraudulent Use*.

Recommendation #1: *State should develop a process and schedule for periodically reassessing security features in the design of its travel documents.*

See comment 1.

**Comment:** The State Department has an informal process in place for periodically reassessing security features in the design of its travel documents and is developing a schedule for periodically reassessing security features in the designs of passports and visas. Under this schedule, at least one assessment will take place every five years.

Recommendation #2: *State should establish a comprehensive oversight program of passport acceptance facilities.*

See comment 2.

**Comment:** Prior to this recommendation, State had already initiated a plan to establish better oversight of passport acceptance facilities. A Program Analyst (GS-13) with considerable project management experience was recently hired to design and implement this comprehensive Acceptance Agent oversight program. This oversight program will improve the performance, integrity, and accountability of the Acceptance Agent Program. The oversight program will:

- Create standards for acceptance agent designation;
- Manage, track, document, train, and better communicate with the Acceptance Agents;
- Improve the quality of incoming passport application packets; and
- Work with the U.S. Postal Service to make passports more trackable by expanding the tracking system to the intake stage.

Recommendation #3: *DHS and State collaborate to provide CBP inspection officers with better training for the inspection of travel documents issued by the State department, to better utilize the security features.*

**Comment:** For future travel documents, the State Department will ensure that exemplars and information on all security features are available to both the ICE-



FDL and CBP-FDAU so that these DHS offices will have sufficient time to produce training materials before the new documents start appearing at ports-of-entry.

In addition, State's Foreign Service Institute (FSI), housed at the George P. Shultz National Foreign Affairs Training Center, offers a full range of in-person and distance-learning training courses on passport and visas that may also respond to this concern. DHS officers, and indeed all officers of the foreign affairs community, can enroll in FSI consular courses, including some that address passport and visa security feature issues. Such interaction is not only a vehicle for DHS officers to receive the latest information on passports and visas, it can also foster more contact between DHS and State officers.

Footnote 6 on p. 8-9: *"DHS and State have indicated that they will begin to implement the [passport] requirement for land and sea ports as early as January 2008."*

See comment 3.

**Comment:** On June 20, 2007, DHS and State jointly announced the next phase of WHTI, governing land and sea ports of entry through a Notice of Proposed Rulemaking (NPRM). The exact implementation date will be determined based upon a number of factors, including the progress of DHS and State actions to implement WHTI and the availability of WHTI-compliant documents on both sides of the border. We expect the date of full implementation will be as early as the summer of 2008. The precise date will be formally announced with at least 60 days notice to the public. The State Department expects to begin issuing passport cards in Spring 2008.

Sentence on p. 14: *"State operates 17 domestic passport-issuing offices, where most passports are issued each year."*

See comment 3.

**Comment:** While it is true that the vast majority of passports are issued in the domestic passport agencies, it should be noted that consular officers also issue to American citizens abroad the Emergency Photo-Digital Passport (EPDP), which went into service in June 2006. The EPDP is a twelve-page emergency U.S. passport intended to replace the previous generation of emergency passports. Although the EPDP is not an "E-passport" and it has no circuitry in it, it brings a new standard of security to emergency passports issued abroad. The EPDP incorporates a digital image of the bearer, biodata, and a machine-readable zone (MRZ) printed on a foil inserted and laminated into a blank book.

Footnote “b” to Table 2 on p. 18: *“Validity Period and Numbers in Circulation, by Passport”*: *“About 140,000 passports were issued to U.S. citizens living overseas prior to April 2002 or as an emergency passport prior to August 2006. After April 8, 2002, overseas passports issuance for U.S. citizens residing or traveling abroad requiring issuance of a U.S. passport was transferred to the National Passport Center in Portsmouth, NH, except for those requiring urgent travel.”*

See comment 3.

**Comment:** The footnote should clarify that all overseas passport applications are adjudicated by consular officers at U.S. embassies and consulates. Both the National Passport Center in Portsmouth as well as the Charleston Passport Center in Charleston, South Carolina, are responsible for printing the non-emergency regular passport books and ensuring that they are sent to the original issuing U.S. posts overseas for distribution. Emergency passport books – the EPDPs – are adjudicated and printed overseas by the issuing posts.

Footnote 16 on p. 20: *“State began the Biometric Visa Program on October 2004.”*

See comment 3.

**Comment:** The first overseas post issued a biometric visa in September 2003. All posts were issuing them by October 2004.

Heading on p. 25: *“State Does Not Have a Structured Process for Periodically Reassessing and Planning for New Generation of Passports and Visas”*

Sentence on p. 26: *“Although State has recently enhanced some of the security features and introduced new security features to the passport, State, for the documents it issues, does not have a policy for reassessing the design’s resistance to evolving counterfeit and alteration threats and planning for new generations of travel documents.”*

Sentence on p. 26-27: *“A structured process for periodically reassessing the security features in documents and planning for new generations should include a policy for reassessing the ability of the document design to resist compromise and fraudulent attempts to the documents.”*

See comment 1.

**Comment:** The three passages quoted above are indicative of a theme of the draft report that a lack of a systematic and formal review process of travel document security features is a border security weakness that needs to be addressed. As a broad response, State recognizes the usefulness of having a more structured

process in place to respond to specific compromises and challenges to security features in travel documents. However, it should be noted that the Bureau of Consular Affairs has a long history of analyzing counterfeit and forged passports and visas with a view toward creating more resistant future versions.

A robust, but informal, process is in place whereby consular officers in the Passport Office and the Office of Fraud Prevention Programs (FPP) track reports from the field of attempts to alter and counterfeit U.S. travel documents. One of the most effective tools that consular officers have is the power to instantly verify any U.S. passport or visa through the Consolidated Consular Database (CCD). A worldwide network of Consular Fraud Prevention Managers regularly pass information and samples (as the report acknowledges on pages 25-26) to State on the latest fraud trends that impact passport and visa security features.

FPP also directly identifies new types of fraudulent documents. In 2001, for example, the first very high quality *Passport '94* counterfeit-page book was intercepted on the U.S. southern border. Port-of-Entry officers mistakenly identified the passport as a routine photo-substitution, and passed it to the local Diplomatic Security office. Eventually, the passport was forwarded to FPP. At that point, it was recognized as a significant fraudulent document. Both FPP and the Forensic Document Laboratory produced alerts on this forgery.

FDL-ICE and CBP-FDAU are indeed important sources of intelligence on fraudulent documents as noted in the draft report. A third source, documents intercepted overseas by foreign immigration services or airlines, is just as important. FPP periodically reminds overseas posts to request that foreign governments return any U.S. travel documents confiscated from mala fide travelers. These documents are eventually passed to FPP for review and some have yielded important intelligence.

For instance, the first known version of a *Passport '98* counterfeit-page book was the result of an interception in Japan. More recently, versions used by Chinese of an improved counterfeit of the same document surfaced. These books contained a counterfeit data page, and often one or more completely counterfeit internal pages. The first book that had all fraudulent internal pages was detected in 2006. This document was intercepted overseas but not identified as being particularly significant until FPP examined the passport. Again, FPP passed this information (and an exemplar) to the FDL which generated an intelligence alert based upon CA's information.

While State agrees there is value in a mandated regular review procedure of document integrity, the creation of such a process is not a substitute for constant vigilance and for responding to vulnerabilities quickly and effectively as they are discovered, or in detecting and preventing fraudulent applications before any passport or visa is wrongly issued.

Sentences on p. 26: *“According to a State [sic], information received on the fraudulent use of passports and visas is reviewed largely on a case specific basis. Moreover, data on this information is not collected or analyzed by State in order to identify counterfeit or alteration trends in attacking the design of the documents.”*

**Comment:** Significant counterfeiting or alteration attempts against passport and visa integrity are closely monitored and analyzed by FPP. Because the quality and methods of these attacks often vary enormously in effectiveness, they do not easily lend themselves to statistical summary. However, State acknowledges the usefulness of keeping trend data.

A major challenge in border security is not only in the protection of the integrity of the travel documents against counterfeiting or alteration, but also the fight to ensure that mala fide travelers do not obtain genuinely issued documents. The draft report rightly acknowledges that most reported passport and visa fraud is tied to imposters who attempt to use genuine documents, not to the physical integrity of the travel documents per se (p. 12). Indeed, imposters and mala fide travelers who have obtained genuine documents may be our greatest challenge, as an analysis of the travel records of the 9/11 terrorists and most other foreign terrorists indicate.

In this context, State believes the report does not provide much consideration to the value of the “forward defense” provided by a system of Fraud Prevention Managers (FPMs) that the Bureau of Consular Affairs has deployed in virtually all domestic passport agencies and consular sections overseas. These FPMs are in regular coordination with the Department through the Passport Services Directorate and the Office of Fraud Prevention Programs. Yet, the report makes little reference to the considerable number of cases these FPMs have foiled through aggressive fraud prevention work. With regard to visas, the data below indicate how many fraud cases FPMs have dealt with through the third quarter of FY 2007. (It should be noted that these statistics reflect a recently introduced metric function feature in the CCD that is still being technically refined. If anything, it understates worldwide fraud prevention activity.)

Visa Fraud Prevention Data in FY 2007 (through 6/30)

Non-Immigrant Visas (NIV) applications

Total Suspected Fraud Cases:	11,846
Fraud Confirmed:	3,024
Fraud Not Confirmed:	7,067
Pending Cases:	1,755

Immigrant Visas/Diversity Visas (IV/DV) applications

Total Suspected Fraud Cases:	7,062
Fraud Confirmed:	1,335
Fraud Not Confirmed:	1,869
Pending Cases:	3,858

Few, if any, of these cases involved an attack against the integrity of the document security features, but represented attempts to obtain a genuinely issued U.S. visa.

Sentence on p. 26: *“For example, although the BCC has been in circulation for almost 10 years, State currently does not have any plans for reassessing the BCC’s features or planning for a new BCC, according to State officials.”*

**Comment:** The comment in the draft report is inaccurate. State is currently redesigning the next generation of the BCC for deployment in 2008 when the current BCCs begin to expire. The new BCC will be modeled after the passport card under development by the Department and will contain a vicinity-read Radio Frequency Identification chip to meet the operational needs of DHS at ports of entry. The next generation BCC will have entirely new artwork design and will incorporate the same cutting-edge security features, including laser engraved photos, as the passport card to mitigate the risk of counterfeiting and forgery. This generation of BCCs will be produced by the Department.

Sentence on p. 31: *“These changes were made to improve State’s ability to combat international parental child abduction, but the measures have also helped prevent or deter identity theft-related fraud in passport applications, according to State officials.”*

**Comment:** State also made these changes to comply with related statutory requirements.

See comment 4.

See comment 3.

Sentence on p. 33: *“Although resources and other tools are available to passport examiners at domestic passport offices...”*

**Comment:** State notes that the same fraud prevention tools are available to consular officers at overseas posts.

Sentence on p. 40: *“In addition, officers who use the databases to inspect State-issued travel documents told us that access to information on visas issued by State has greatly improved their ability to reliably confirm the validity of visas and detect their fraudulent use.”*

Sentence on p. 41: *“At secondary inspection, CBP officers have more time and greater access to inspection-related technologies and equipment, and thus are more capable of confirming the fraudulent use of U.S. passports and visas identified at primary inspection.”*

**Comment:** State believes the text cited above, while accurate, should more fully detail the value of the Consular Consolidated Database (CCD) to CBP officers in the fight to maintain border security. The CCD contains not only the Department’s worldwide visa records, but the Passport Information Electronic Retrieval System (PIERS), enabling CBP officers at secondary to verify any visa or passport issued within the past decade. CCD records also provide detailed individual biographic application information and applicant photos.

Updated around the world every five minutes, the CCD typifies the maxim that *“information is power,”* demonstrating again why data sharing is one of the best tools in the U.S. Government’s arsenal to protect our borders. The CCD is particularly useful in helping to detect forgeries and altered travel documents. Biometric features in the CCD are also useful in countering imposters who are using genuine documents.

Sentence on p. 48: *“Some ports are equipped with photophones to transmit images of documents to FDL experts for verification of altered and counterfeit U.S. passports and visas, and secondary officers can forward suspected fraudulent U.S. passports and visas to FDL experts for a thorough forensic examination.”*

**Comment:** The process described in the sentence above does not reflect the state of the art at secondary inspection in confirming fraud. As noted above, during

secondary inspection, CBP officers can confirm a suspect visa or passport's authenticity through a fast check in the CCD.

Sentences on p. 49: *“Although State began issuing e-passports as early as December 2005, CBP was not provided with e-passport exemplars in March 2007, according to State documentation. According to CBP officials, training on the features of the new e-passport was not provided to officers at basic training until April 2007.”*

**Comment:** State's Passport Services Directorate is developing a program for the issuance and distribution of passport exemplars. Previously, distribution responsibilities were shared between Passport Services and FPP. With regard to the new e-passport, Passport Services and FPP divided the duties. Passport Services distributed exemplars to the foreign embassies in Washington, and FPP distributed them to domestic partner agencies and to overseas Foreign Service posts for use with foreign governments.

FPP officers traveled to the Federal Law Enforcement Training Center (FLETC) in Georgia in October 2006 and February 2007 to provide training to the DHS Fraud Detection and National Security officers. On both those occasions, new passport exemplars were given to host DHS training officials for use in their own training.

It is worth noting that in basic principle, the concept of a passport is primarily to communicate information from the issuing government to other governments of countries to which the bearer may travel. The passport also serves as a means of communication from one agency of the issuing government to another. It is not inappropriate to prioritize the distribution of information about a new passport design to representatives of foreign governments. It should also be noted that the Department began issuing the e-passport to the public in August 2006. The Department issued only diplomatic and official e-passports prior to August 2006 to test them in the DHS/CBP operational environment at select ports-of-entry with the full knowledge and cooperation of DHS/CBP.

---

The following are GAO's comments on the Department of State's letter dated July 24, 2007.

---

## GAO Comments

1. We believe there is value in a mandated regular review procedure for document integrity and recommend that State develop a process and schedule for periodically reassessing security features in the design of its travel documents. We recognize that an informal process is important for responding to vulnerabilities and counterfeit or altered passports and visas, as they are discovered. It is not our intention to inhibit or replace the informal process already in place. However, we believe that an informal process by itself is not an effective way to re-evaluate the security features of passports and visas against evolving counterfeit and alteration threats. While State has made adjustments in the design of passports and visas, its approach has been largely reactive. A structured process for reassessing the features and planning for new generations of passports and visas is critical because counterfeit and alteration threats to the security of these documents are always changing, many passports and visas have a long lifespan, and it takes State several years to fully implement a new document design. The increasing pace of technology change and use of electronics makes State's current approach less viable than it might have been in the past, and best practices, such as for currency design, suggest that periodic evaluation of designs and introduction of new security features are more viable approaches in the management of counterfeit and alteration threats. We welcome State's recent steps to develop a schedule for periodically reassessing security features in the design of passports and visas.
2. We welcome State's recent steps to hire an analyst to design and implement a comprehensive program for the oversight of passport acceptance agents. During the course of our review, we were informed that the acceptance agent program remained a significant fraud concern and that efforts were under way to implement actions to address identified vulnerabilities in this program. However, State officials were unable to provide us with documentation identifying these vulnerabilities or a plan for addressing them. After our draft report was provided to the agency for review and comment, we were provided with a draft document identifying initiatives to improve oversight of the passport acceptance agent program. State has identified the vulnerabilities in this program and proposed reasonable oversight measures to address these vulnerabilities.
3. We revised the text of this report to reflect this information.



- 
4. During the course of our review, we were informed by Consular Affairs officials in the Office of Fraud Prevention Programs that State did not have a formal process for reassessing the security features in visas or for planning the redesign of the documents in the future. According to these officials, formal plans for redesigning the BCC did not exist, although they did indicate that State was considering the use of the new passport card design to develop the next BCC. We welcome the decision to model the new BCC after the passport card design and issue the next generation of this card in 2008, when the current cards will begin to expire. Furthermore, we believe it is important to periodically reassess the security features in the design of the new BCC to manage future counterfeit and alteration threats.

# Appendix VII: Comments from the Department of Homeland Security

Note: GAO comments supplementing those in the report text appear at the end of this appendix.

U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

July 20, 2007

Jess Ford  
Director, International Affairs and Trade  
U.S. Government Accountability Office  
Washington, DC 20548

Dear Mr. Ford:

Thank you for the opportunity to review and comment on the Government Accountability Office's (GAO) report titled "BORDER SECURITY: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use" GAO-07-1006SU.

The report addresses 1) the features of U.S. passports and visas and how information on these features is shared; 2) the integrity of the issuance process; and 3) how these documents are inspected at U.S. ports of entry.

The following is our response to the recommendations that pertain to the Department of Homeland Security (DHS).

#### Recommendation 3

Develop a deployment schedule for providing sufficient e-passport readers to U.S. ports of entry, which would enable inspection officials to better utilize the security features in the new U.S. e-passport.

Response: Concur.

CBP is working to make US Passport issuance data and photographs available during the primary inspection process to improve the security of not only US e-passports but also all US issued passports. By allowing CBP Officers expanded use of the Consular Consolidated Database (CCD), access to US passport application and issuance information can be done directly from the system of record. This enhancement would provide CBP Officers, at time of inspection, the passport photograph and associated biographic data that can be directly compared to the photograph and biographic data printed within the passport. It is important to note that the Department of State has already made US Passport information accessible to CBP for use in CBP secondary locations.

[www.dhs.gov](http://www.dhs.gov)

**Appendix VII: Comments from the  
Department of Homeland Security**

CBP fully intends to develop and deploy e-passport readers to all U.S. ports of entry to ensure our ability to verify e-passports from all countries. However, the e-passport technology is still new and the readers are not yet ready for full deployment. DHS is continuing to work with vendors to improve e-passport technology and to incorporate it into all lanes once the readers are technically ready and funding is available.

Due Date July 2008

**Recommendation 4**

Develop a strategy for better utilizing the biometric features of the BCC in the inspection process to reduce risk of imposter fraud.

Response: Concur.

CBP agrees with the goal of increasing biometric verification for foreign nationals. The US-VISIT capability available today at airport and seaport on primary and at secondary for land enables CBP officers to biometrically compare and authenticate travel documents issued to non-US Citizens by DHS and State (e.g. Border Crossing Cards (BCC), Nonimmigrant (NIV) and Immigrant (IV) Visas, Permanent Resident Cards, Reentry Permits, Refugee Travel Documents). CBP is reviewing the requirements and cost of deploying this US-VISIT capability at all pedestrian primary locations as well.

Today, CBP Officers, after swiping the Machine Readable Zone (MRZ), are presented biographic issuance data and a photograph that they compare against the document presented and the traveler. The photograph and biographic data display provide immediate document alteration identification, which directly reduces the risk of imposter fraud. In addition, CBP Officers collect fingerprints that are being compared by the system to the fingerprints on file, using automation to ensure the individual presenting the document is the one to whom it was issued. Fingerprints are currently collected routinely for those presenting NIVs (including those using a BCC as a B1/B2 visa) or those traveling under the Visa Waiver Program. US-VISIT has published a proposed regulation that would expand the current biometric collection procedures to all classes of aliens, other than Canadian B1/B2.

CBP is developing a strategy whereby RFID-enabled travel documents, including future RFID-enabled BCC, can be used to pre-position biographic issuance and photographic information to CBP officers processing travelers in possession of such documents – eliminating the need to swipe the card on the land borders.

As a final note, CBP has recently re-issued to all field personnel our passenger primary inspection procedures to ensure uniform and consistent processing.

Due Date Complete

**Recommendation 5**

We are recommending that the Secretaries of State and DHS collaborate to provide CBP inspection officers with better training for the inspection of travel documents issued by the State department, to better utilize the security features. This training should include:

See comment. 1.

---

**Appendix VII: Comments from the  
Department of Homeland Security**

---

Training materials that reflect changes to State-issued travel documents in advance of State's issuance of these documents, including the provision of exemplars of new versions of these documents in advance of issuance.

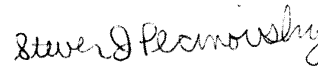
Response: Concur.

CBP will initiate discussion with the State Department to ensure all future new or revised State-issued travel documents are made available to CBP in sufficient quantity for field officer training prior to introduction for public use. CBP will follow with production of a training module to be provided to CBP field offices with exemplars of the new document. Specifically, planning efforts are already underway to ensure that CBP officers will receive training on the proposed Passport Card, due for issuance by State beginning in 2008, in a timely manner.

In addition, CBP will formulate a working group with the State Department Offices of Passport Services and Consular Affairs, to include representation from their Fraud Prevention Program. The purpose of the group will be to evaluate recent fraud trends in State Department issued documents and to prepare training material for dissemination to field offices.

Due Date: The working group will meet a minimum of every six months, with the initial meeting taken place by August 31, 2007. The proposed Passport Card is due for issuance by State in the beginning of 2008.

Sincerely,



Steven J. Pecinovsky  
Director  
Departmental GAO/OIG Liaison Office

---

The following are GAO's comments on the Department of Homeland Security's letter dated July 20, 2007.

---

## GAO Comment

1. We agree that DHS's US-VISIT capability enables primary inspectors at air and some sea ports of entry to use the fingerprint biometric to compare and authenticate the document and holder of visas and BCCs. However, at land border ports this capability is not available in primary inspection. Travelers with BCCs at southern land border ports—the ports where BCC imposter fraud is most significant—are not routinely referred to secondary inspection, where they do have the capability to utilize the fingerprint records for comparison. In addition, at southern land border ports, all BCCs are not machine-read for access to the biographic data and photo during primary inspection and vehicle lanes do not have the capability to access the photograph for comparison. As a result, inspectors are not making full use of the biometric information available for BCCs. To more fully utilize the available fingerprint biometric in the BCC and mitigate imposter fraud, we are suggesting that DHS develop a strategy to better use both fingerprint biometric of the BCC and increase card reads of the BCC in primary inspection at southern land border ports of entry.

---

# Appendix VIII: GAO Contact and Staff Acknowledgments

---

## GAO Contact

Jess T. Ford, (202) 512-4268 or [fordj@gao.gov](mailto:fordj@gao.gov)

---

## Staff Acknowledgments

In addition to the contact named above, John Brummet (Assistant Director), Claude Adrien, Monica Brym, Joe Carney, Richard Hung, and Bradley Hunt made key contributions to this report. Technical assistance was provided by Kate Brentzel, Aniruddha Dasgupta, Etana Finkler, Elisabeth Helmer, Sona Kalapura, Chris Martin, Jose Pena, and Marisela Perez.

---

## GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

---

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site ([www.gao.gov](http://www.gao.gov)). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to [www.gao.gov](http://www.gao.gov) and select "Subscribe to Updates."

---

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are \$2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office  
441 G Street NW, Room LM  
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000  
TDD: (202) 512-2537  
Fax: (202) 512-6061

---

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: [www.gao.gov/fraudnet/fraudnet.htm](http://www.gao.gov/fraudnet/fraudnet.htm)

E-mail: [fraudnet@gao.gov](mailto:fraudnet@gao.gov)

Automated answering system: (800) 424-5454 or (202) 512-7470

---

## Congressional Relations

Gloria Jarmon, Managing Director, [JarmonG@gao.gov](mailto:JarmonG@gao.gov) (202) 512-4400  
U.S. Government Accountability Office, 441 G Street NW, Room 7125  
Washington, D.C. 20548

---

## Public Affairs

Paul Anderson, Managing Director, [AndersonP1@gao.gov](mailto:AndersonP1@gao.gov) (202) 512-4800  
U.S. Government Accountability Office, 441 G Street NW, Room 7149  
Washington, D.C. 20548