

~~**SENSITIVE BUT UNCLASSIFIED**~~

**United States Department of State
and the Broadcasting Board of Governors
Office of Inspector General**

Office of Audits

**Safeguarding Domestic
Passport Applications
During Transit**

Report Number AUD/IP-08-19, March 2008

~~**IMPORTANT NOTICE**~~

~~This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

~~**SENSITIVE BUT UNCLASSIFIED**~~



**United States Department of State
and the Broadcasting Board of Governors**

Office of Inspector General

PREFACE

This report was prepared by the Office of Inspector General (OIG) pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its responsibility to promote effective management, accountability and positive change in the Department of State and the Broadcasting Board of Governors.

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

The recommendations therein have been developed on the basis of the best knowledge available to the OIG and, as appropriate, have been discussed in draft with those responsible for implementation. It is my hope that these recommendations will result in more effective, efficient, and/or economical operations.

I express my appreciation to all of those who contributed to the preparation of this report.

A handwritten signature in black ink, appearing to read "H. W. Geisel".

Harold W. Geisel
Acting Inspector General

TABLE OF CONTENTS

EXECUTIVE SUMMARY	1
BACKGROUND	5
OBJECTIVES, SCOPE, AND METHODOLOGY	11
RESULTS	15
Phased-in Mandates Increase Demand for U.S. Passports	15
The Number of Lost Passport Applications Is Increasing	17
Controls Established Prior to FY 2007	18
Applications Were Not Always Safeguarded at Acceptance Agent	
Facilities	19
Mailed Passport Applications Cannot Be Tracked	21
Transportation Routing Increases Risk of Losing Passport Applications ..	23
Areas Are Not Always Secure at USPS Mail Distribution Center	24
Access Within Passport Agencies Is Not Restricted	25
Management Corrective Actions Taken or Underway During FY 2007 ...	28
Management Action Is Needed To Clarify OIG Access Authority	29
LIST OF RECOMMENDATIONS	33
ABBREVIATIONS	35
APPENDICES	
A. CA/PPT Passport Agencies	37
B. FY 2007 Passport Applications Reported by CA/PPT as Lost	39
C. Example of Passport Application Routing: Culver City, CA, Lockbox ..	
Facility to East Coast Passport Agencies	41
D. Department Comments – The Bureau of Consular Affairs	43

EXECUTIVE SUMMARY

A passport is an official government document that certifies an individual's identity and citizenship and permits a citizen to travel abroad. Only the U.S. Department of State (Department) has authority to issue U.S. passports. To obtain a passport, U.S. citizens are required to complete an application and provide supporting documentation that contains personally identifiable information (PII), such as an applicant's birth or naturalization certificate. The Department is committed to maintaining the integrity of the U.S. passport and is responsible for safeguarding passport applications. During FY 2007, the Department issued nearly 18.4 million passports.

Recognizing the need to safeguard highly sensitive personal information and to prevent its unauthorized use, the Office of Inspector General (OIG) initiated this audit to determine whether domestic passport applications were adequately safeguarded during transit. During the audit, the Bureau of Consular Affairs, Office of Passport Services (CA/PPT), finalized guidelines¹ that outline the actions it should take when applications are lost. Depending on the scenario, CA/PPT would notify outside authorities, including officials in the Department of the Treasury, the Department of Homeland Security, and the United States Postal Service (USPS). OIG will address the Department's compliance with these new external reporting requirements for lost PII in subsequent audits.

In November and December 2006, the Department reported a total of 1,156 domestic passport applications and their supporting identification documents had been lost in transit in three separate incidents—752 of these were found later. As of October 26, 2007, the Department reported that there had been 14 additional incidents in FY 2007 involving 333 lost application packages, 46 of which were found. However, the number of passport applications reported as still missing compared with the number of passports issued in FY 2007 was less than one one-hundredth of a percent (691 out of 18.4 million) and proportionally insignificant.

Safeguarding PII in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public.

OMB Memorandum M-07-16,
“Safeguarding Against and Responding
to the Breach of Personally Identifiable
Information”

¹ Missing Application Guidelines, November 8, 2007.

OIG's recommendations should help the Department reduce the risk of missing applications and increase its ability to track the applications throughout the transportation and processing processes. This, in turn, should decrease the likelihood that highly sensitive personal information contained in passport applications could be used for criminal purposes, such as identify theft. OIG met with CA/PPT officials on December 13, 2007, to discuss its findings. These officials agreed with the audit results and said that further improvements are needed to safeguard passport applications. In response to OIG's draft report, CA generally concurred with OIG's recommendations and has begun implementing corrective actions. (See Appendix D.)

BACKGROUND

Only the Department has authority to issue passports to U.S. citizens.² Within the Department, CA/PPT is responsible for issuing passports to U.S. citizens. Through 18 passport agencies across the United States, CA/PPT processes domestic passport applications, prints passport books, and provides information and services to American citizens on how to obtain, replace, or change a passport. (The 18 CA/PPT passport agencies are listed in Appendix A.)

PASSPORT APPLICATION PROCESS

The Applicant

To obtain a passport, a U.S. citizen must complete an application by providing two photographs and present a previous passport or proof of citizenship, such as a birth certificate or a naturalization certificate. Applicants must then pay appropriate processing fees according to the fee schedule as follows:

- Passport execution: Required for first-time applicants and others who must apply in person³ \$30
- Passport application services for:
 - (a) Applicants age 16 or over (including renewals) \$55
 - (b) Applicants under age 16 \$40
 - (c) Passport amendments (such as extension of validity and name change) No Fee
- Passport security surcharge (required for all applicants) \$12
- Expedited service: guaranteed 3-day processing and/or in-person service at a U.S. passport agency (not applicable abroad) \$60

² 22 U.S.C 211a.

³ Acceptance facilities, including the Department's passport agencies, execute passport applications on the Department's behalf and retain this fee. Execution tasks include mailing applications to the Treasury's lockbox.

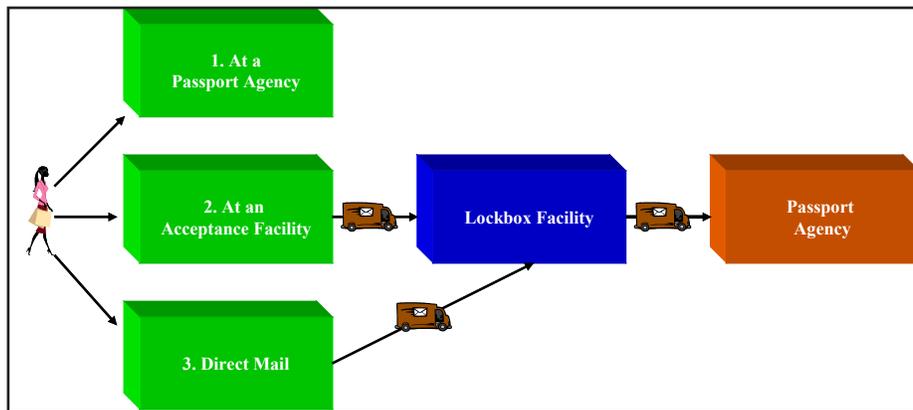
First-time applicants also have to take an oath affirming the information on the application is true and correct.

Domestically, completed applications are submitted to CA/PPT in three ways:⁴

- An applicant may apply in person at 15 of the 18 passport agencies⁵ across the country.
- An applicant can apply at any of the over 9,000 acceptance facilities, such as a USPS post office.
- For renewals only, an applicant may mail the passport application to either of two official lockbox facilities.

The passport application process is depicted in Figure 1.

Figure 1: Domestic Passport Application Process



Source: OIG

Acceptance Agents and Distribution Facilities

For applications not submitted at a passport agency, several key agents and entities are involved in the passport application process and are responsible for safeguarding passport applications while in their possession.⁶ These include acceptance agents; USPS; the Department of the Treasury’s financial agent lockbox facilities; state, county, township, or municipal offices; and other public entities such as libraries. Although CA/PPT does not have direct control over safeguarding passport applications while they are in the custody of these other entities, it is responsible for

4 Passport application requirements for U.S. citizens living overseas are not addressed here or in Figure 1 and were not reviewed as a part of this audit.
5 Three of these passport agencies are used exclusively for processing applications or passport book printing and are not open to the public.
6 5 U.S.C. 552a.

establishing policies and procedures for the application acceptance and transportation process to be used by these entities and for monitoring compliance with its requirements.

Acceptance agents must be U.S. citizens or nationals and authorized by CA/PPT to accept passport applications at over 9,000 acceptance facilities throughout the country. Responsibilities of acceptance agents include verifying whether an applicant's identification documents, such as a driver's license, actually match the applicant. These responsibilities are detailed in CA/PPT's Passport Application Acceptance Program, which is designed to provide information on acceptance agent qualifications and requirements, as well as an overview of the application acceptance process.

Applications accepted at acceptance facilities are routed to USPS and Treasury lockbox facilities for further processing. USPS uses its Los Angeles, CA, and Philadelphia, PA, mail distribution centers to accumulate and presort passport applications destined for the lockbox facilities in Culver City, CA, and New Castle, DE, respectively. The lockbox facilities are in financial institutions designated as financial agents by the Treasury. The Los Angeles and Philadelphia centers sort application packages received from acceptance facilities and individuals throughout the country. Passport applications are sorted either by expedited or routine processing and are then further separated by passport agency destination. Once the applications are sorted, they are placed within labeled hampers and staged for pickup by designated couriers.

Passport applications mailed by acceptance facilities and individual applicants are addressed to one of the two lockbox facilities. The lockbox facility verifies the completeness of the passport application packages received, which includes processing fee payments and batching passport applications. The batched passport application packages are then transported to passport agencies based on CA/PPT's weekly distribution notification to the lockbox facility. During FY 2007, the lockbox facility received and transported approximately 16.7 million (90 percent) passport application packages of 18.6 million received. (See Appendix A for the Treasury's lockbox facilities.)

Shipments to Passport Agencies

Each week CA/PPT, using a workload distribution analysis, determines the number of applications each lockbox facility will ship to a particular passport agency for adjudication and issuance. Workload distribution is calculated based on statistics of the prior week (such as workload capacity and labor or administrative circumstances) provided by CA/PPT's Field Operations Group. This analysis helps the smaller

passport agencies maintain a consistent level of service while not exceeding their processing capacity. Application overflows are routed to the major passport agency processing centers in Portsmouth, NH; Charleston, SC; and New Orleans, LA. These workload transfers were particularly important during FY 2007 because of the large number of applications CA/PPT received during the fiscal year.

LAWS, REGULATIONS, AND GUIDANCE ON SAFEGUARDING PASSPORT APPLICATIONS

The Federal Government has set forth requirements to protect PII⁷ that apply to safeguarding information contained in passport applications. In addition, the Department and CA/PPT have issued written guidance on passport applications. The governing laws, regulations, and guidance relating to passport applications are listed in Table 1.

Table 1. Governing Laws, Regulations, and Guidance for Passport Applications

General Federal Requirements	
The Privacy Act	This law mandates agencies to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained. (5 U.S.C. 552a)
OMB Memorandum M-07-16, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."⁸	This memorandum requires agencies to: <ul style="list-style-type: none">• Establish safeguards to ensure the security and confidentiality of records, and• Protect against any anticipated threats or hazards to their security or integrity that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained.

⁷ The term "personally identifiable information," as defined by the Office of Management and Budget, refers to information that can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth and mother's maiden name.

⁸ Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft, May 10, 2006

Department Requirements for Passport Agencies	
Foreign Affairs Manual (FAM)	<p>The FAM is the source for the organizational structures, policies, and procedures that govern the operations of the Department; the Foreign Service; and, when applicable, other Foreign Affairs agencies. (2 FAM 1111.2(b)) Key policies with respect to this audit include the following:</p> <ul style="list-style-type: none">• Access to and use of records by employees are subject to the determination of a need-to-know by offices responsible for the information. (5 FAM 471)• An individual's passport information is identified as Sensitive But Unclassified (SBU) information. All SBU information is required to be handled, processed, transmitted, and stored in means that limit the potential for unauthorized disclosure. (12 FAM 544)
Bureau of Consular Affairs Internal Controls Program Standards	<p>The Internal Controls Program identifies and addresses areas of vulnerability, with the overall goal of maintaining strict accountability of passport books, money, and adjudicative decision-making at passport agencies. Key requirements include the following:</p> <ul style="list-style-type: none">• Passport applications in process should be locked up overnight.• Free access to passport agencies is restricted only to authorized personnel.• Unauthorized personnel include cleaning crews and delivery persons.• Cleaning crews should not be allowed unescorted access to the work area.

OBJECTIVES, SCOPE, AND METHODOLOGY

In December 2006, a Treasury OIG official reported to OIG's hotline an incident involving 752 lost applications. (See Appendix B, incident #1.) While looking into this first incident, OIG learned that a total of 1,156 applications had been lost⁹ in transit in three separate incidents from November through December 2006. Because of increasing concerns in the United States to protect PII, OIG initiated this audit to determine whether domestic passport applications were adequately safeguarded during transit. OIG's planned review to determine whether the Department had complied with requirements in reporting the loss of PII will be addressed in subsequent audits.

Although 691 applications received during FY 2007 were still missing as of October 26, 2007, these lost applications were a proportionally small number, representing less than one one-hundredth of a percent of the 18.4 million passports issued. CA/PPT officials said they took action to notify applicants regarding the missing applications and offered free credit monitoring service. However, OIG did not independently verify these actions or determine whether CA/PPT had complied with requirements in reporting a loss of PII. OIG plans to review PII during other audit engagements.

OIG reviewed the following five steps involved in the domestic passport application process:

- (1) Acceptance agents accept passport applications from customers.
- (2) Acceptance agents send the application packages to the Treasury's lockbox facilities.
- (3) The lockbox facilities sort, batch, scan, and screen the application packages.
- (4) Couriers deliver the packages to passport agencies.
- (5) Passport agencies receive and store the applications for adjudication.

OIG performed its work primarily at the Bureau of Consular Affairs headquarter

9 OIG considers a passport application "lost" when it cannot be located.

ters in Washington, DC; four passport agencies;¹⁰ one lockbox facility;¹¹ one mail distribution center;¹² and five acceptance facilities.¹³ Site visits were performed at these facilities in May and June 2007 and work included interviewing officials, reviewing passport applications and related information, observing the processing of passport applications, evaluating transportation plans for sending applications to passport agencies, and accessing controls for safeguarding passport applications.

In addition, OIG reviewed and analyzed OIG inspection reports, Government Accountability Office (GAO) audit reports, and applicable laws and regulations. OIG also reviewed CA/PPT officials' congressional testimony regarding passport applications, interviewed Bureau of Diplomatic Security (DS) officials about passport agency building security requirements, and met with USPS and Treasury officials to discuss their policies and procedures for handling passport applications. OIG audited applications processed during FY 2007. Older information from previous fiscal years was obtained but not audited.

OIG did not investigate the reported incidents of the lost passport applications, but it did rely on reports by other entities that had investigated some of the incidents. OIG also did not conduct data reliability or verification tests for the information provided by CA/PPT and the lockbox regarding the number of passports issued since FY 2002.

OIG performed its fieldwork from April to November 2007. OIG conducted this performance audit in accordance with generally accepted government auditing standards. These standards require that OIG plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objectives. OIG believes the evidence obtained provides a reasonable basis for the findings and conclusions based on its audit objectives.

On December 13, 2007, OIG discussed the audit findings with CA/PPT officials. CA/PPT officials agreed with the audit results and said that further improve-

10 Passport facilities visited were the passport agencies in Boston, MA; Philadelphia, PA; Washington, DC; and the National Passport Center in Portsmouth, NH.

11 The lockbox facility visited was in New Castle, DE. The lockbox facility was moved to a complex in Newark, DE, as of November 2007.

12 The mail distribution center visited is in Philadelphia, PA.

13 Acceptance facilities visited were USPS post offices in Merrifield, VA; Philadelphia, PA; and Portsmouth, NH. Also visited were the City of Takoma Park, MD, and the Annapolis Circuit Court Clerk in Annapolis, MD.

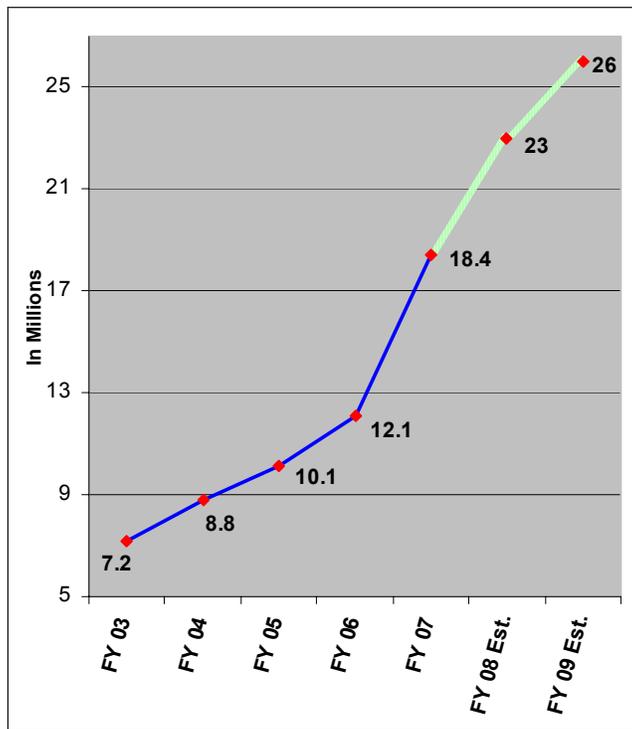
ments are needed to safeguard passport applications. OIG also provided a discussion draft of its audit results to USPS and Treasury officials on December 19, 2007. Treasury and USPS officials provided comments on December 26, 2007, and January 8, 2008, respectively. OIG clarified portions of its draft report as appropriate based on the comments provided.

OIG provided a copy of the draft report to CA on January 23, 2008, and to USPS and the Treasury on February 6, 2008. On February 19, 2008, CA provided formal comments to the draft report, which are incorporated where applicable and included in their entirety as Appendix D. On February 14, 2008, the Treasury provided informal comments that requested further clarifications regarding the governing documents over the lockbox provider and the relationships between CA/PPT, the Treasury, the lockbox provider, and the package delivery contractor. These clarifications have been incorporated where applicable.

document that establishes the bearer’s identity and nationality to enter or depart the United States from within the Western Hemisphere. This travel initiative is being implemented in two phases. The first phase, which began on January 23, 2007, will be for air travel, and the second phase, which begins on January 31, 2008, will be for land and sea travel.

Because of these mandated requirements, the demand for U.S. passports has increased significantly since FY 2005, when 10.1 million passports were issued. In FY 2007, CA/PPT issued nearly 18.4 million passports to U.S. citizens, or more than an 80 percent increase in the number of passports issued in FY 2005. (See Figure 2.) In addition, CA/PPT predicts that the demand will continue to rise and estimates that the Department will issue 23 million passports in FY 2008 and 26 million in FY 2009.

Figure 2. Domestic Passports Issued for FYs 2003-07 and Estimated for FYs 2008–09

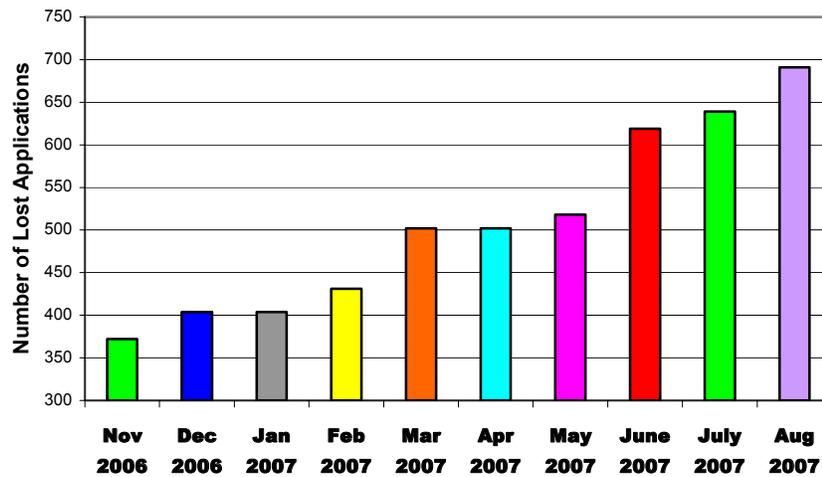


Source: OIG chart based on CA/PPT data as of October 17, 2007.

The Number of Lost Passport Applications Is Increasing

The cumulative number of lost applications has increased during FY 2007, as shown in Figure 3. From November through December 2006, there were three reported incidents of lost passport applications involving 1,156 passport applications.¹⁷ However, 752 of these applications were located before OIG announced its audit in March 2007. During the audit, CA/PPT reported 14 more incidents involving 333 lost passport applications, of which 46 applications were found. As of October 26, 2007, 691 of the total 1,489 lost passport applications had not been found. (See Appendix B for details on passport applications reported as lost in FY 2007.)

Figure 3. Outstanding Lost Domestic Passport Applications by Month (Cumulative)



Source: OIG chart based on CA/PPT incident data as of October 26, 2007.

¹⁷ An incident is when one or more passport applications being transported at the same time cannot be located.

Controls Established Prior to FY 2007

CA/PPT has an existing system of internal controls over passport applications as required by FAM and the Office of Management and Budget (OMB). (See “Department Requirements for Passport Agencies” in Table 1.) These controls include having physical security at processing facilities, requiring clearances for CA/PPT and lockbox facility personnel, segregating duties for processing applications, and reconciling passport applications.

Passport agencies and lockbox facilities had numerous physical security controls. For example, at the passport agencies OIG visited, individuals were required to go through metal detectors before they entered the facility, security guards monitored customers waiting in line for service, passport agency doors had ciphered locks, and protective glass shields were located where adjudicators provided service to customers. At the lockbox facility OIG visited, security staff were observed walking the premises and monitoring deliveries, keeping access doors locked when mail was not being received, and having couriers sign in before they entered the facility.

Personnel at lockbox facilities are required to have security background checks, and personnel at passport agencies are required to have security clearances. Access to lockbox facilities and passport agencies is limited to those individuals who have met personnel security requirements. Lockbox employees undergo initial and annual security awareness training. In addition, new employees must attend a security orientation within 10 business days of arriving at the lockbox.

Lockbox facilities and passport agencies segregate their duties for processing passport applications. For example, separate lockbox personnel are assigned to sort, open, screen, and compile the applications. Other lockbox personnel re-screen, review, scan, batch, reconcile, and pack the applications for shipment to the passport agencies. At the passport agencies, personnel separately open, scan, and adjudicate documents in the application package. Other staff print passport books and perform quality control checks before mailing passports to applicants.

Both lockbox facilities track the screened passport applications through to delivery at passport agencies. Lockbox employees place a bar code sticker on each application and, if the package contains a prepaid envelope, write a tracking number on the application. Screened passport applications are reconciled by lockbox personnel before they are transported to the passport agencies. Once the applications are ready for dispatch at the lockbox, an employee packs boxes with a packing slip identifying the batched applications and makes certain that the number of applications in each

batch matches the number on the packing slip. If there is a discrepancy, lockbox personnel will check whether all applications have been scanned. If applications have been scanned but cannot be located, lockbox personnel will notify CA/PPT headquarters of the incident. The lockbox provides the passport agency with an electronic shipping report, which details the number of passport applications scheduled for shipment before the package delivery contractor makes its delivery.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Acceptance Agent Facilities

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)

While CA/PPT does not have direct control over applications in the possession of the acceptance agents, it does provide acceptance agents general information and instructions on passport applications in its Passport Agent’s Reference Guide (PARG). (See “Department Requirements for Acceptance Facilities” in Table 1.)

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) Acceptance agents are prohibited by the PARG from releasing passport application information to anyone other than the applicant and CA/PPT and from retaining copies of completed applications.

18 The Passport Agent’s Reference Guide, October 2007, Chapter 10, section 6.

In its response, the Bureau of Consular Affairs concurred with the recommendation and stated that it will add a monitoring component and application security to the acceptance agent oversight program currently being developed. The Bureau of Consular Affairs said the current “Site Visit Checklist” contains an item to check that applications, documents, and fees are securely maintained and that it will ensure the inclusion of application security in its expanded oversight program. On the basis of the Assistant Secretary’s response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives a copy of the acceptance agent oversight program detailing provisions for monitoring the effectiveness of acceptance agents in securing passport applications.

(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)
(b) (2)(b) (2)

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)(b) (2)(b) (2)

(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)
(b) (2)(b) (2)

20 The Passport Agent’s Reference Guide, October 2007, Chapter 10, section 6.

for the passports, CA/PPT has made or plans to make changes in how it processes passport applications. CA/PPT has:

- Set up helpdesk and adjudication taskforces to increase the processing of passport applications (these taskforces include volunteers from several Department bureaus).
- Expanded its processing operations, which includes opening a facility that exclusively prints passport books.
- Increased its capacity to hold passport applications in process, such as by adding storage annexes to existing buildings.

CA/PPT also has aggressively recruited staff because of the increased demand for passports. CA/PPT hired almost 500 government and contract employees in May and June 2007, and approximately 550 candidates are being processed for potential employment as direct-hire adjudicators.

Management Action Is Needed To Clarify OIG Access Authority

OIG found that the Department had not notified acceptance agents about OIG's authority to review passport-related records. OIG also found that the PARG and a sample designation letter included in CA/PPT's Passport Application Acceptance Program information packet did not include language making acceptance agents aware of OIG's authority.

In contrast, the Treasury has a provision that expressly describes OIG's authority and access to lockbox facilities. Included in the Invitation for Expressions of Interest (IEI) that governs the operations of lockbox facilities (see "Treasury and Department Requirements for Lockbox Facilities" in Table 1), this provision, entitled "Inspection Personnel," states:

Special Agents and other auditors representing the investigative and program review functions of the U.S. Treasury Office of the Inspector General (OIG), respectively, should be granted staff-like access after proper authentication of IDs by the [financial agent]. The OIG, per the Inspector General Act of 1978, should receive full cooperation of the QLP [qualified lockbox provider] in support of the OIG's broad investigative and audit powers related to (a) determining whether programs are achieving intended results and in compliance with governing laws and regulations, and (b) identifying fraud, waste, and abuse. This is applicable to other government auditors (e.g., GAO) and/or their designated independent audit agencies or firms.

Also, the Federal Acquisition Regulation (FAR)²⁹ requires all federal contracts to contain a clause that requires contractors to make available records such as books, documents, accounting policies and practices, and other data, regardless of type and regardless of whether such items are in written form, in the form of computer data, or in any other form, and other supporting evidence to satisfy contract negotiation, administration, and audit requirements of the contracting agencies. Even though acceptance agents are not contractors, this clause or the IEI provision could be a model for guidance for the acceptance agents.

Although many OIG requests are related to specific audits, OIG may also need immediate access to passport records in emergency situations such as those involving stolen or destroyed applications, as demonstrated by an incident reported by CA/PPT that occurred in Algona, WA.

The Seattle Passport Agency in Algona reported on July 18, 2007, that an employee of the City of Algona acceptance facility was suspected of having stolen or destroyed 22 passport applications that were dated from February to May 2007. A report was filed with the Algona Police Department (one of the missing applications was for the Chief of Police for Algona), and the employee was placed on administrative leave. This situation was discovered when the employee went on vacation in May 2007, and customers made inquiries concerning their applications. DS completed its investigation and presented the case for federal prosecution. The City of Algona has suspended passport operations while the situation is under investigation. The applications have not been found.³⁰

Because of incidences such as the preceding, CA/PPT should notify acceptance agents of the OIG's authority over and access to all passport records.

Recommendation 7: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to issue an advisory notice within 14 days of the issuance of this audit report to all acceptance agents informing them of the Office of Inspector General's authority to review passport records as specified in the Inspector General Act.

In its response, the Bureau of Consular Affairs stated it will issue a notice to all acceptance agents regarding this recommendation. On the basis of the Assistant Secretary's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives a copy of the notice.

²⁹ 52 FAR 215.2.

³⁰ Incident #12 as reported by CA/PPT.

Recommendation 8: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the Passport Agent's Reference Guide to require agents to make their passport records available for monitoring, audit, or investigation.

In its response, the Bureau of Consular Affairs concurred with the recommendation and stated that it will make this change in the calendar year 2008 update to the PARG. On the basis of the Assistant Secretary's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives a copy of the updated PARG containing this modification.

Recommendation 9: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the provisions in the designation letter to make passport records available for monitoring, audit, or investigation and reissue the designation letter for all acceptance agents.

In its response, the Bureau of Consular Affairs concurred with the recommendation. However, it proposed combining the notification requirements from recommendations 1, 7, and 9 in a notice to all acceptance agents, identifying the content as resulting from the final version of this OIG report. On the basis of the Assistant Secretary's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives a copy of the notice to all acceptance agents.

LIST OF RECOMMENDATIONS

Recommendation 1: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the PARG to define the minimum standards for a secure area, (b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) and issue a notice to all acceptance agents regarding this change.

Recommendation 2: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to include provisions in its acceptance agent oversight program for monitoring the effectiveness of acceptance agents in securing passport applications.

Recommendation 3: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 4: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to work with officials from the Department of Treasury to review the process used to transport passport applications from the lockbox facilities to passport agencies and to develop a workload distribution analysis that reduces the use of routes with numerous transfers.

Recommendation 5: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 6: (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

Recommendation 7: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to issue an advisory notice within 14 days of the issuance of this audit report to all acceptance agents informing them of the Office of Inspector General's authority to review passport records as specified in the Inspector General Act.

Recommendation 8: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the Passport Agent's Reference Guide to require agents to make their passport records available for monitoring, audit, or investigation.

Recommendation 9: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the provisions in the designation letter to make passport records available for monitoring, audit, or investigation and reissue the designation letter for all acceptance agents.

ABBREVIATIONS

CA/PPT	Bureau of Consular Affairs, Office of Passport Services
Department	U.S. Department of State
DHS	Department of Homeland Security
DS	Bureau of Diplomatic Security
FAM	Foreign Affairs Manual
FAR	Federal Acquisition Regulation
GAO	Government Accountability Office
GPS	Global positioning systems
IEI	Invitation for Expressions of Interest
NPC	National Passport Center
OIG	Office of Inspector General
OMB	Office Management and Budget
PARG	Passport Agent's Reference Guide
PII	Personally identifiable information
QLP	Qualified lockbox provider
SBU	Sensitive But Unclassified
SOW	Statement of Work
Treasury	U.S. Department of the Treasury
U.S.C.	United States Code
USPS	United States Postal Service

APPENDIX A

CA/PPT Passport Agencies

	Passport Agencies	Location
1	Boston	Boston, MA
2	Chicago	Chicago, IL
3	Colorado	Aurora, CO
4	Connecticut	Norwalk, CT
5	Honolulu	Honolulu, HI
6	Houston	Houston, TX
7	Los Angeles	Los Angeles, CA
8	Miami	Miami, FL
9	New Orleans	New Orleans, LA
10	New York	New York, NY
11	Philadelphia	Philadelphia, PA
12	San Francisco	San Francisco, CA
13	Seattle	Seattle, WA
14	Washington	Washington, DC
15	Special Issuance ¹	Washington, DC
16	Charleston Passport Center ²	Charleston, SC
17	National Passport Center ²	Portsmouth, NH
18	Arkansas Passport Center ³	Hot Springs, AR

¹ The Special Issuance Agency handles passport issuance for U.S. Government travelers and other special cases.

² These two Passport Centers are used exclusively for processing applications and are not open to the public.

³ This Passport Center is used exclusively for printing passport books.

Department of Treasury Lockbox Facilities

	Lockbox Facilities	Location
1	Culver City	Culver City, CA
2	Newark	Newark, DE

United States Postal Service Mail Distribution Centers

	Mail Distribution Centers	Location
1	Philadelphia	Philadelphia, PA
2	Los Angeles	Los Angeles, CA

APPENDIX B

FY 2007 Passport Applications Reported by CA/PPT as Lost

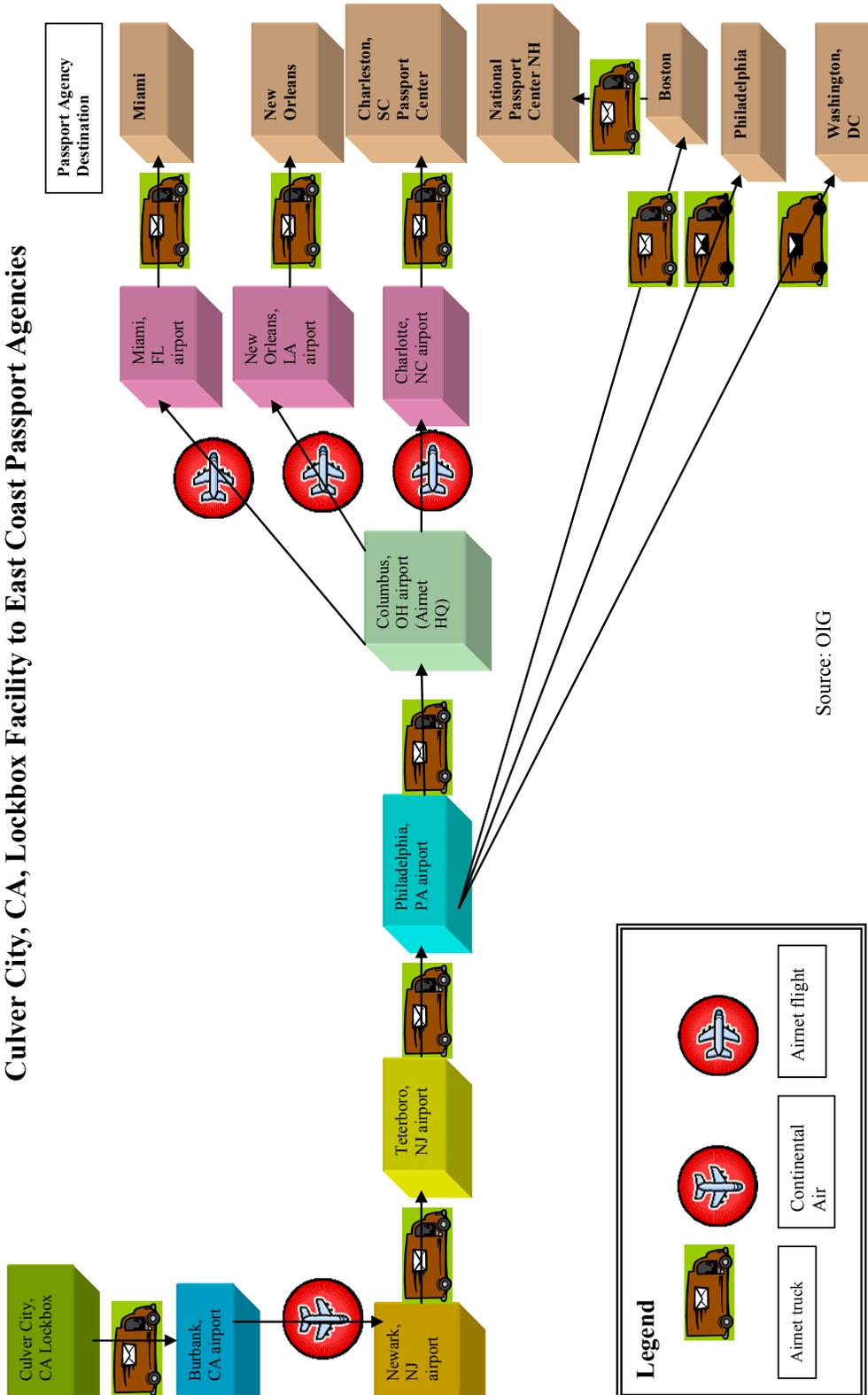
Incidents	Date of Incident	Date Reported to CA/PPT	Number of Applications Lost	Location Where Last Seen	Date Found	Where Found	Number Found	Number of Days Missing Since Reported
1	12/2/2006	12/4/2006	752	Airport	12/22/2006	Airport	752	18
2	12/14/2006	12/19/2006	32	Lockbox	Not Found	---	---	311
3	11/28-30/2007	12/30/2006	372	Mail Distribution Center	Not Found	---	---	300
Before Audit Subtotal (#1-3)			1,156				752	
4	Early March 2007	3/20/2007	23	Lockbox	Not Found	---	---	220
5	2/3/2007	4/9/2007	27	Non-Postal Courier Driver	Not Found	Stolen	---	200
6	3/16/2007	4/25/2007	25	Passport Agency	5/9/2007	Passport Agency	25	14
7	3/19/2007	5/4/2007	10	Lockbox	6/22/2007	Lockbox	10	49
8	5/25/2007	5/25/2007	1	Lockbox	Not Found	---	---	154
9	6/4/2007	6/4/2007	32	Unknown	Not Found	---	---	144
10	5/2/2007	6/19/2007	11	Acceptance Facility	6/22/2007	Acceptance Facility	11	3
11	5/17/2007	6/22/2007	7	Acceptance Facility	Not Found	---	---	126
12	2/9/07 - 5/14/07	7/18/2007	22	Acceptance Facility	Not Found	---	---	Varying dates
13	3/16/2007	8/6/2007	13	Lockbox	Not Found	---	---	81
14	6/6/2007	Unknown	90	Lockbox	Not Found	---	---	Unknown
15	7/3/2007	Unknown	19	Passport Agency	Not Found	---	---	Unknown
16	7/8/2007	9/27/2007	1	Acceptance Facility	Not Found	---	---	29
17	8/15-31/2007	10/5/2007	52	Lockbox	Not Found	---	---	21
During Audit Subtotal (#4-17)			333				46	
Total			1,489				798	
Total Applications Still Lost			691					
Percentage of Applications Lost			0.004%					

NOTE: The number of days missing since reported was calculated by subtracting the date of the incident from the date the last incident report was received from CA/PPT. If the passport applications were found, then the date of the incident was subtracted from the day the applications were found.

Source: OIG table based on CA/PPT data as of October 26, 2007.

APPENDIX C

**Example of Passport Application Routing:
Culver City, CA, Lockbox Facility to East Coast Passport Agencies**



APPENDIX D



United States Department of State

*Assistant Secretary of State
for Consular Affairs*

Washington, D. C. 20520

SENSITIVE BUT UNCLASSIFIED

INFORMATION MEMO TO ACTING INSPECTOR GENERAL TODD - OIG

FROM: CA - Maura Harty

SUBJECT: Draft Audit Report, *Safeguarding Passport Applications During Transit* (AUD/08-XX), dated January 23, 2008

Attached is CA's response to your office's January 2008 Draft Audit Report on *Safeguarding Passport Applications during Transit*. We appreciate your insights, and CA is well on the way to implementing your recommendations. I am confident that these improvements will enhance the security of the passport application process. My staff is prepared to answer any additional questions at anytime. The Bureau point of contact is Barry Conway, Director, Office of Passport Integrity and Internal Controls; he can be reached at 663-2430.

Attachment:

CA Responses to Draft Audit Report, *Safeguarding Passport Applications During Transit* (AUD/08-XX), dated January 23, 2008

"Safeguarding Domestic Passport Applications During Transit"

CA's Response to Recommendations

Recommendation 1: The Office of the Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the PARG to define the minimum standards for a secure area, (b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) and issue a notice to all acceptance agents regarding this change.

CA's Response: As noted in the Draft Report, the Office of Passport Services (PPT) added the language, "in a safe and secure location until mailed daily," to the PARG in October 2007. In addition, PPT added a pictorial flow that includes (b) (2) (b) (2)(b) (2)(b) (2) applications. CA will add language in the next PARG update that also puts the picture into words. CA will issue a combined notice to all acceptance agents that will include change/notification items from Recommendation 1, 7, and 9.

Recommendation 2: The Office of the Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to include provisions in its acceptance agent oversight program for monitoring the effectiveness of acceptance agents in securing passport applications.

CA's Response: CA concurs with this recommendation and will add a monitoring component to the acceptance agent oversight program currently being developed. One of the key tenets of the program will be the development of a database which will allow PPT to assign identification numbers to each acceptance facility and track data on facility performance and training. With this information, PPT will be able to track the performance of the acceptance facility and identify trends and needs for additional training. Further, the current *Site Visit Checklist*, contains seven items in the "Security" section, one of which is, "Applications, Documents, and Fees Securely Maintained; no non-essential access." In addition, CA will ensure the inclusion of application security in its expanded oversight program.

Recommendation 3 (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2) (b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)(b) (2)

CA's Response: CA concurs with the recommendation; however, there are practical concerns that must simultaneously be addressed. (b) (2)(b) (2)

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

4

To further ensure that Agencies are securing access, dissemination and release of information we have in place additional safeguards including the following:

- All persons entering facilities must display their identification badge per the 12 FAM 370 regulations.
- Entry and exit to restricted areas is monitored by armed guards and secured by card or "buzz in" access only.
- Lockers are provided to staff to store bags and personal items to ensure that SBU material is not removed from the building. Where lockers cannot be made available given space and layout restrictions, bags are reviewed by guards before exiting secured areas. When possible, both activities occur upon exit from a secured area.

During non-working hours, PPT also maintains information per the regulations in accordance with 12 FAM 544.1 .d which states the following:

"During non duty hours, SBU information and removable electronic media in US. -Government facilities must be secured with a locked office or suite, or secured in a locked container".

Compliance is ensured as all information is maintained within a locked and guarded agency.

In addition to securing applications, PPT takes additional steps to ensure the security of books, ribbons and foils, as well as applicant fees. Chapter Four of our ICG discusses each of these items and the specific steps necessary to secure them.

Recommendation 7: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services. to issue an advisory notice within 14 days of the issuance of this audit report to all acceptance agents informing them of the Office of Inspector General's authority to review passport records as specified in the Inspector General Act.

CA's Response: CA will issue a combined notice to all acceptance agents that will include change/notification items from Recommendations 1, 7, and 9.

Recommendation 8: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the Passport Agent's Reference Guide to require agents to make their passport records available for monitoring, audit, or investigation.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

5

CA's Response: CA concurs and will make the change in the second calendar year 2008 PARC update.

Recommendation 9: The Office of Inspector General recommends that the Bureau of Consular Affairs direct the Office of Passport Services to modify the provisions in the designation letter to make passport records available for monitoring, audit, or investigation and reissue the designation letter for all acceptance agents.

CA's Response: CA concurs; however, reissuing letters of designation would require individualizing letters. As a more expedient approach and perhaps, one with even greater impact, CA proposes to combine notification requirements from Recommendations 1, 7, and 9 in a notice to all acceptance agents, identifying the content as resulting from the final version of this OIG Report. While fully recognizing OIG authority for access to all Department of State records, we suggest that OIG continue to notify PPT in advance (whenever possible) of plans to visit acceptance facilities, so that we can assist to ensure access is readily granted.

SENSITIVE BUT UNCLASSIFIED

FRAUD, WASTE, ABUSE OR MISMANAGEMENT
of Federal programs
and resources hurts everyone.

Call the Office of Inspector General
HOTLINE
202/647-3320
or 1-800-409-9926
or e-mail oighotline@state.gov
to report illegal or wasteful activities.

You may also write to
Office of Inspector General
U.S. Department of State
Post Office Box 9778
Arlington, VA 22219
Please visit our website at oig.state.gov

Cables to the Inspector General
should be slugged "OIG Channel"
to ensure confidentiality.