



**U.S. DEPARTMENT OF THE INTERIOR
OFFICE OF INSPECTOR GENERAL**

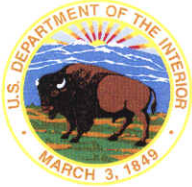
INSPECTION REPORT



**PASSPORT OFFICES FAILING TO MANAGE AND
SECURE EMPLOYEE PASSPORTS**

REPORT NO. ER-EV-MOA-0002-2008

MAY 2009



United States Department of the Interior

Office of Inspector General
Washington, DC 20240

MAY 19 2009

Memorandum

To: Secretary Salazar

From: Mary L. Kendall
Acting Inspector General

Stephen A. Hoffmann
for

Subject: Final Report — Passport Offices Failing to Manage and Secure Employee
Passports (Report No. ER-EV-MOA-0002-2008)

This memorandum transmits our report detailing lapses in security of diplomatic and official passports issued to employees who travel internationally on behalf of the Department of the Interior (DOI or Department). We conducted a series of unannounced inspections at the three Department offices that manage passports, the National Business Center (NBC), the U.S. Geological Survey (USGS), and the Bureau of Reclamation (BOR). We refer to these offices collectively as the Passport Offices. The purpose of our inspection was to determine whether DOI has collected passports from separating employees and disposed of them appropriately and secured passports, visas, and passport applications in accordance with federal and Departmental regulations.

We noted that at least 49 former DOI employees may still have possession of valid official passports that identify them as representatives of the U.S. Government. The seriousness of this issue is highlighted by the example of DOI not recovering the official passport of a former DOI employee later convicted of a felony. We also found thousands of valid and expired passports, visas, and passport applications that were not appropriately secured or accounted for in DOI's Passport Offices. In short, the Passport Offices have committed multiple violations of the Privacy Act, the Departmental Manual, and other federal regulations. Given the risk of misuse that missing and unsecured passports, visas, and passport applications pose, we cannot understate the importance of acting swiftly to address these violations and prevent their recurrence.

This report contains seven recommendations to improve accountability and security of these sensitive documents. We would appreciate being kept apprised of the actions DOI takes on our recommendations as we will track the status of their implementation. We request that NBC, USGS, and BOR provide written responses to this Office within 30 days that identify plans to address the findings and recommendations cited in this report.

Should you have any comments or questions regarding this report, please do not hesitate to contact me at 202–208–5745.

cc: Assistant Secretary, Land and Minerals Management
Assistant Secretary, Water and Science
Assistant Secretary, Policy, Management, and Budget
Deputy Assistant Secretary for Passport Services, Department of State
Acting Inspector General, Department of State

PASSPORT OFFICES FAILING TO MANAGE AND SECURE EMPLOYEE PASSPORTS

TABLE OF CONTENTS

Introduction.....	1
DOI Cannot Account for Dozens of Passports Held by Former Employee.....	3
Violations Abound in DOI Passport Offices.....	4
Document Management.....	4
Storage	4
Disposal and Retention.....	6
Tracking.....	6
Training	7
Conclusion	7
Recommendations	8
Appendices	
Scope, Methodology, and Prior Reviews	A
Passport Security Requirements	B

CIAL PORT



States
merica

INTRODUCTION

The U.S. passport is arguably the most coveted travel document in the world. Required of U.S. citizens for international travel and re-entry into the Country, the passport serves as official verification of the bearer's origin, identity, and nationality. Each day, Americans submit passports as identification to board domestic flights, obtain licenses to drive, apply for loans, and verify their employability status.

The most recognizable passport, the blue-cover tourist passport, is used to travel overseas for pleasure or to conduct private business. However, the U.S. Department of State (State) issues two additional types of passports, diplomatic and official. A *diplomatic passport* is carried by a federal employee or contractor who has been granted the privilege of diplomatic status overseas. An *official passport* identifies the bearer as a federal employee or contractor who represents the U.S. Government in an official capacity abroad; it does not convey diplomatic status. At DOI, only the Secretary of the Interior holds a diplomatic passport, while all other employees traveling overseas carry official passports.



The Office of Inspector General estimates that there are over 3,000 valid passports issued to current employees. These individuals fulfill a wide variety of duties overseas to advance the Department's mission. For instance, DOI's International Technical Assistance Program, established in cooperation with the U.S. Agency for International Development, has sent DOI employees to assist 25 countries to date. These staff provide skills and knowledge in fields such as endangered species conservation, invasive species control, and fire and water resource management. For other employees, travel abroad constitutes an integral part of their regular duties. For example, a number of U.S. Fish and Wildlife Service (FWS) inspectors work along the Nation's borders with Canada and Mexico and routinely enter those countries. In addition, the Office of Insular Affairs regularly sends employees overseas to monitor grant funds provided to the Federated States of Micronesia, the Marshall Islands, and Palau under the Compacts of Free Association.

To facilitate the issuance of passports, the Code of Federal Regulations (CFR), in 22 C.F.R. § 51.22(b), authorizes State to designate certain individuals as passport acceptance agents. The CFR details their responsibilities as:

- certifying the identity of and administering an oath to passport applicants;
- safeguarding passport application information; and
- avoiding a real or perceived conflict of interest with regard to the passport process.

Currently, 10 DOI employees serve as passport acceptance agents. Beyond the duties outlined in the CFR, these individuals are responsible for submitting completed applications to State, distributing executed diplomatic and official passports to employees, obtaining any required visas from foreign embassies, storing passports not needed by travelers, reporting lost or missing passports to State, and returning passports to State after employees separate from DOI. The passport acceptance agents are based in one of three DOI offices. These are the:

- NBC Employee and Public Services Division (this office processes passport and visa requests for all DOI offices and bureaus except BOR and USGS);
- USGS International Programs Office in Reston, VA; and
- BOR Native American and International Affairs Office located in Washington, DC, and Denver, CO.

Diplomatic and official passport records maintained by these three offices are subject to the Privacy Act of 1974. To protect the privacy of U.S. citizens, the Privacy Act places limitations on agencies' collection, disclosure, and use of personal information maintained in systems of records, such as passport and visa files. According to the Privacy Act, when agencies establish or make changes to a system of records, they must notify the public by placing a notice in the "Federal Register." These notices are a primary means of establishing accountability for privacy protections (see 64 FR 16981 (April 7, 1999) for DOI's notice). They identify, among other things, the type of data collected, the location of the records, and information on how the data are disposed of and secured.



The NBC Passport Office in Washington, DC, manages the passport and visa process for all other DOI employees. NBC has two full-time passport acceptance agents.



The USGS International Programs Office, located in Reston, VA, employs five collateral-duty passport acceptance agents. One additional position was vacant at the time of our inspection.



The BOR Native American and International Affairs Office, located in Washington, DC, and Denver, CO, employs three collateral-duty passport acceptance agents.

DOI CANNOT ACCOUNT FOR DOZENS OF PASSPORTS HELD BY FORMER EMPLOYEES


The Passport Offices were unable to account for 49 expired passports, at the time of our review that were either missing or checked out to former employees. This number could be much higher because, unlike USGS and BOR, NBC has no passport database and could not provide us with a comprehensive list of valid passports. Since our initial visits in February, USGS and BOR have collected passports from some separated employees and forwarded them to State for cancellation. While we applaud USGS and BOR for taking action immediately, DOI needs to do much more to ensure that departing employees return their official passports.

The wide ranging examples we found involve passport holders from the highest ranks of the Department to lower-ranking staff from a number of DOI's bureaus and offices. For example, the NBC Passport Office cannot locate former Secretary of the Interior Gale Norton's diplomatic passport, which expires in 2010. Ms. Norton resigned 3 years ago and completed an employee exit clearance form at that time. All employees must complete these forms to ensure that they return all Government property and fulfill their financial obligations prior to leaving DOI. An NBC employee signed Ms. Norton's form indicating that the passport had been returned without actually receiving the passport. The NBC Passport Office was unable to tell us whether Secretary Norton's diplomatic passport was returned to State.

In addition, two former employees — a felon convicted after departing DOI and a high-level official who was investigated for ethics rules violations while working at DOI — ostensibly neglected to return their official passports to the NBC Passport Office (see below). We found no evidence that NBC asked State to cancel these passports, which remained valid for months after the employees left DOI. We found that their official passports are missing from their files in the NBC Passport Office.

- Milton K. Dial, a former MMS employee, pled guilty to the felony charge of arranging a contract for a former colleague who hired him 6 months after his retirement from DOI. His official passport expired in February 2009, more than 4 years after he left federal service and approximately 4 months following his guilty plea.
- David P. Smith, a former Fish, Wildlife, and Parks employee, was investigated twice during his tenure at DOI for violating ethics standards. His official passport expired in April 2007, 9 months after his resignation.

According to passport acceptance agents at NBC, USGS, and BOR, they are responsible for passports but have no control over the Department's checkout procedures. They have to trust that current employees will return their passports between trips and that separating employees will return their passports to the appropriate Passport Office. Furthermore, the Passport Offices



are not always informed in advance of an employee's separation so that an agent can obtain the departing employee's passport for return to State for cancellation. As they stand, the checkout procedures are not effective and need to be improved.

VIOLATIONS ABOUND IN DOI PASSPORT OFFICES

During our inspections of the Passport Offices, we observed numerous violations of federal and Departmental requirements governing security of passports, visas, and passport applications (see Table 1.) In the absence of Departmental oversight, responsibility for protecting sensitive documents and information has devolved to the bureaus. All of the Passport Offices function autonomously; none functions properly.

While the problems vary across each of these offices, in general, we found a combination of inadequate resources, a lack of understanding of security requirements for passports, and an inability to track passports. These conditions have resulted in the improper storage, retention, tracking of passports, visas, and applications, and inadequate protection of Privacy Act information.

Document Management

Storage

In 64 FR 16981 (April 7, 1999), DOI informed the public that it keeps passport and visa records in steel safes with manipulation-proof, three-way combination locks. We found, however, that the NBC and USGS Passport Offices store passports and visas in filing cabinets that are lockable only by key. The NBC Passport Office also stored over 400 expired passports in an unlocked drawer (see photograph on page 6). Furthermore, approximately 200 files containing passport applications and expired passports were stacked on unsecured shelves and spilled onto the floor just inside the entrance to the NBC Passport Office. These files were readily accessible to unauthorized personnel. (See report cover.)

Requirement	BOR	NBC	USGS
Were passports stored in steel safes with three-way combination locks?	YES	NO	NO
Were all passport applications stored in a locked cabinet or drawer?	NO	NO	NO
Were valid passports consistently obtained from employees prior to separation?	NO	NO	NO
Was the Department of State notified of all valid passports retained by former employees?	NO	NO	NO
Upon expiration, were all passports returned to the Department of State for cancellation?	NO	NO	NO
Were the required Privacy Act notices posted?	YES	NO	NO

Table 1. Violations of Federal and Departmental Requirements Governing Security of Passports, Visa, and Passport Applications

Further, none of the Passport Offices afforded passport applications the same level of security as passports, even though the personal information contained in completed applications (mother's maiden name, social security numbers, and addresses) is more sensitive than that in passports. A case involving State illustrates the ease with which identities can be stolen using information gleaned from passport applications. Specifically, an incident in Washington, DC, in October 2008 prompted State to notify approximately 400 passport applicants of a breach in its database security. Police officers had stopped a vehicle and found 21 credit cards in names other than the driver's and printouts of eight completed passport applications. Four of the names on the passport applications matched names on the credit cards. Investigation revealed that the driver worked with co-conspirators at State and the U.S. Postal Service.

In fact, none of the DOI Passport Offices stored all of their passport applications in a locked safe, cabinet, or drawer. According to the Departmental Manual (383 DM 8.2), bureaus should implement more stringent safeguards for systems of records containing particularly sensitive information than the minimum required because the sensitivity of such information may vary from one system of records to another.

We were unable to determine the locations of all DOI-maintained official passports. According to 64 FR 16981, passports and visas are kept only at the NBC Passport Office; however, we found thousands of passports stored in the BOR Passport Office in Washington, DC, and at USGS Headquarters in Reston, VA. The USGS and BOR Passport Offices are not listed in

64 FR 16981, as required. We also discovered that FWS stored passports in offices near the U.S./Canadian border; we were unable to obtain the addresses of those offices. Without a comprehensive list of all locations where passports are kept, DOI managers and Privacy Act officers cannot effectively manage these records or ensure that diplomatic and official passports are secured appropriately.



This photograph shows over 400 expired passports stored in an unlocked drawer in the NBC Passport Office.

Disposal and Retention

General Records Schedule (GRS) Number 9, which is cited in 64 FR 16981, requires that each official passport be returned to State upon expiration or separation of the employee. We found that the USGS and BOR Passport Offices kept expired passports on file and retained passport applications longer than federal regulations allowed. The passport acceptance agents we interviewed were not aware of the GRS requirement.

Furthermore, the Privacy Act itself states that an agency shall maintain in its records only such information as is relevant and necessary to accomplish a purpose of the agency (5 U.S.C. § 552a(e)(1)). In addition, 22 C.F.R. § 51.22(e)(2) prohibits passport acceptance agents from retaining copies of executed passport applications. DOI does not require copies of executed passport applications to effectively carry out its mission. Nevertheless, one BOR passport acceptance agent informed us that she kept copies of completed applications on file for up to 5 years. USGS staff also stated that they retained copies of passport applications for up to 3 years after passports were issued.

Tracking

The Government Accountability Office (GAO) “Standards for Internal Control in the Federal Government” states, “Internal control and all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination. . . . All documentation and records should be properly managed and maintained.” Unfortunately, none of the Passport Offices has an adequate means to track the location and status of official passports or to determine whether passports of separated employees have been returned to State, as required.

For example, NBC has no database; when we asked for information, NBC provided an incomplete list that only included passports processed recently. As a result, NBC could not tell us how many valid passports it manages. In fact, the NBC Passport Office passport acceptance agents could not locate 2 of the 20 passport files we selected for review from their records. To

date, these files, which likely contain Privacy Act information and may even hold the employees' official passports and visas, remain missing.

Training

The July 2007 report titled "Common Risks Impeding the Adequate Protection of Government Information" issued by Department of Homeland Security (DHS) and Office of Management and Budget (OMB) (see Appendix A) identified inadequate training as one of the top 10 mistakes federal agencies make in protecting privacy information. We also found training of DOI passport acceptance agents to be inadequate.

Privacy Act Requirements

Even though passport acceptance agents must be certified by State before assuming their duties and must take DOI's annual Privacy Act training, we found that these individuals are largely unaware of how to protect sensitive information according to regulatory and Departmental requirements (see Appendix B). In fact, NBC and USGS failed to post Privacy Act notices in accordance with the Departmental Manual (383 DM 8.3A). Areas where Privacy Act information is stored should be posted with warnings regarding access limitation, standards of conduct for employees handling such information, and possible criminal penalties for violations. In fact, none of the Passport Offices store passports and passport-related documents in accordance with the Act — contrary to DOI's assertions in 64 FR 16981 (April 7, 1999).

Passport Acceptance Agent Refresher Courses

The current regimen of training given by State is also inadequate to ensure appropriate handling of passports by acceptance agents and their supervisors over the long-term. One passport acceptance agent stated that she completed the required training to become an agent in 1999. She has not had a refresher course on handling passports and passport-related documents since that time.

To address training inadequacies, DHS and OMB included best practices in their July 2007 report. We believe a number of those practices would benefit the Passport Offices. Specifically, training could be 1) tailored to address the requirements of the Passport Offices in terms of passport acceptance agent roles and responsibilities, 2) given upon hiring and at least once a year thereafter, and 3) assessed regularly for its effectiveness and modified as requirements change. Such training would exceed the standard annual Privacy Act training; it would encompass all Privacy Act, federal, and Departmental requirements that pertain to the handling and protection of passports and passport-related documents (see Appendix B).

CONCLUSION

DOI and the Passport Offices are failing in their responsibility to collect passports from departing employees, as well as to dispose of them properly, and to ensure proper storage, retention, and handling of passports and passport applications. Their mismanagement and inadequate protection of diplomatic and official passports violate law and federal and Departmental regulations. As a result, they have openly invited misuse of U.S. passports; cases of fraud or theft of employee identities could easily result.

RECOMMENDATIONS

By implementing the following recommendations, we believe DOI can address the problems identified in this inspection.

We recommend that the Secretary direct the Department to:

1. Issue a revision of 64 FR 16981 to accurately reflect the location of the passport offices and to update any other items that might be in error or outdated.
2. Issue a revision of 383 DM 8.3B to be consistent with the standards laid out in 64 FR 16981 regarding the storage of passports and passport applications.
3. Require that passport acceptance agents undergo regular training on federal and Departmental standards governing the managing and securing of passports and passport-related information (see recommendation 4 below).

We recommend that the Secretary direct NBC, USGS, and BOR to:

1. Develop a process to ensure that passports, visas, and passport applications are stored, retained, disposed of, and tracked in accordance with federal (Privacy Act) and Departmental regulations. Particular attention should be paid to making sure employees return their diplomatic and official passports to DOI before separating and notifying State of any uncollected passports.
2. Destroy passport applications once State issues the corresponding passports.
3. Post Privacy Act notices clearly wherever passports, visas, and passport applications are stored.
4. Consult with State regarding the provision and content of regular training to DOI passport acceptance agents on federal and Departmental standards that govern the managing and securing of passports and passport-related information.

SCOPE, METHODOLOGY, AND PRIOR REVIEWS

The objective of our inspection was to determine whether DOI has collected passports from separating employees, as well as disposed of them appropriately and secured passports, visas, and passport applications in accordance with federal and Departmental regulations.

We conducted this inspection from January to March 2009, in accordance with the “Quality Standards for Inspections” issued by the President’s Council on Integrity and Efficiency. To accomplish our objectives, we:

- attempted to gain unauthorized access to the NBC and BOR Passport Offices;
- observed the passport application process by submitting an application for an OIG employee who required a passport for official travel;
- performed an unannounced inspection of the BOR, NBC, and USGS Passport Offices on January 29, 2009;
- interviewed passport acceptance agents at the NBC Passport Office in Washington, DC; the USGS Passport Office in Reston, VA, and the BOR Passport Office in Washington, DC, and Denver, CO regarding passport security and the process for disposing of passports;
- selected a sample of 52 DOI passport holders to determine whether the passport acceptance agents could account for these employees’ passports; and
- determined whether employees who separated from DOI before February 1, 2009, returned their diplomatic and official passports prior to leaving the Department.

Prior Reviews

Over the past 5 years, GAO has issued several reports related to the physical security over passports, passport fraud, and protection of Privacy Act information. The following reports were most applicable to our inspection of the DOI Passport Offices:

- **“Addressing Significant Vulnerabilities in the Department of State’s Passport Issuance Process,” Statement of Jess T. Ford, Director, International Affairs and Trade and Gregory D. Kutz, Managing Director, Forensic Audits and Special Investigations, Correspondence to the Senate Committee on the Judiciary (Subcommittee on Terrorism and Homeland Security), Report No. GAO-09-583R, Issued April 13, 2009.** In their correspondence to the Senate, Mr. Ford and Mr. Kutz reported that State Department continues to face significant fraud vulnerabilities in their passport issuance process. They recounted that a GAO undercover investigator easily obtained genuine U.S. passports using counterfeit or fraudulently obtained documents.

Reducing these risks, according to officials at State, will require greater cooperation between State and other agencies at both the federal and state levels, including the need to access electronic records of other agencies in real time.

- **“Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use,” Report No. GAO-07-1006, issued July 2007.** GAO reported that State did not have a structured process to periodically reassess the effectiveness of passports’ security features against evolving threats or to actively plan for new generations of passports. The report also noted that State lacked a program to oversee thousands of passport acceptance facilities, which verify the identity of millions of passport applicants each year. Such a program, according to GAO, would help minimize the risk of passport fraud.
- **“Preventing and Responding to Improper Disclosures of Personal Information,” Statement of David M. Walker, Comptroller General, Before the House Committee on Government Reform, Report No. GAO-06-833T, issued June 2006.** In his testimony, the Comptroller General addressed a security breach at the Department of Veterans Affairs, in which the personal data of millions of veterans were compromised. Although the testimony largely discussed information technology security, the Comptroller General noted that practical measures aimed at preventing inadvertent data breaches include limiting the collection of personal data, limiting the time that such data are retained, limiting access to personal information, and training personnel accordingly.
- **“Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts,” Report No. GAO-05-477, issued May 2005.** GAO reported that State faced a variety of challenges to its passport fraud detection efforts, making it more difficult to protect U.S. citizens from terrorists and criminals. For instance, information listed in the Government’s consolidated terrorist watch list was not systematically provided to State. Furthermore, State did not routinely obtain from the Federal Bureau of Investigation the names of individuals wanted by federal or any of the States’ law enforcement authorities. As a result, the Consular Lookout and Support System database did not contain information on a number of fugitives suspected of murder, child sex offenses, drug trafficking, and other heinous crimes. In addition, GAO noted that State made oversight visits to only a limited number of passport acceptance facilities each year and did not maintain records of all individuals authorized to accept passports at those locations.

We noted one additional report applicable to security over privacy information, which Department of Homeland Security and the Office of Management and Budget prepared in response to a request made by the President’s Identity Theft Task Force:

- **“Common Risks Impeding the Adequate Protection of Government Information,” issued July 2007 by the Department of Homeland Security and the Office of Management and Budget.** This report highlighted 10 “mistakes” commonly made by Government agencies entrusted with security and privacy information. It also detailed best practices and resources to help agencies avoid and mitigate these risks. The common mistakes included: 1) inadequate security and privacy training;

2) missing safeguarding procedures from contracts and data sharing agreements between agencies; 3) inaccurate information inventories that do not correctly describe where information is stored; 4) incorrect or inappropriate scheduling, archiving, or destroying of information; 5) untimely identification and reporting of suspicious activities and security incidents; 6) inadequate or absent audit trails documenting information processing; and 7) insufficient physical security controls over privacy information; 8) inadequate information security controls; 9) insufficient protection of information accessed or processed remotely; and, 10) premature use of information technology and products before application of security and privacy standards and guidelines.

PASSPORT SECURITY REQUIREMENTS

22 CFR § 51.22(e)(2)	<ul style="list-style-type: none">• Passport acceptance agents must not retain copies of executed passport applications.
383 DM 8.2	<ul style="list-style-type: none">• The sensitivity of personal information may vary from one system of records to another. Bureaus should implement safeguards beyond the required minimum for systems of records containing particularly sensitive information.
383 DM 8.3A	<ul style="list-style-type: none">• The area where Privacy Act information is stored should be posted with warnings regarding access limitation, standards of conduct for employees handling such information, and possible criminal penalties for violations.
383 DM 8.3B	<ul style="list-style-type: none">• At all times, access to Privacy Act records should be restricted by storing the records in a locked metal file cabinet or locked room, except when the room is occupied by authorized personnel.
64 FR 16981 (April 7, 1999)	<ul style="list-style-type: none">• Passports and visas are stored in a steel safe with a manipulation-proof, three-way combination lock.• Passports and visas are retained and disposed of in accordance with General Records Schedule No. 9.
General Records Schedule No. 9	<ul style="list-style-type: none">• Official passports should be returned to State upon expiration or upon separation of the employee.

Report Fraud, Waste, Abuse, and Mismanagement



Fraud, waste, and abuse in government concerns everyone: Office of Inspector General staff, Departmental employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and abuse related to Departmental or Insular Area programs and operations. You can report allegations to us in several ways.



By Mail:

U.S. Department of the Interior
Office of Inspector General
Mail Stop 4428 MIB
1849 C Street, NW
Washington, D.C. 20240

By Phone:

24-Hour Toll Free	800-424-5081
Washington Metro Area	703-487-5435

By Fax:

703-487-5402

By Internet:

www.doioig.gov/hotline