

SENSITIVE BUT UNCLASSIFIED

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

Office of Audits

**Review of Controls and Notification for Access to
Passport Records in the Department of State's
Passport Information Electronic Records System (PIERS)**

AUD/IP-08-29

July 2008

Important Notice

This report is intended solely for the official use of the Department of State or any agency receiving the report directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State 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

SENSITIVE BUT UNCLASSIFIED

I. Bureau of Human Resources Response100

J. Foreign Service Institute Response.....102

K. Bureau of Information Resource Management Response104

Background

Congress established the Department of State (Department) as the sole authority to issue passports to U.S. citizens,⁴ and the Bureau of Consular Affairs (CA) is tasked with this responsibility. Through 18 passport agencies across the United States, CA processes domestic passport applications; prints passport books; and provides information and services to U.S. citizens on how to obtain, replace, or change a passport. CA also supports the issuance of passports through embassies and consulates abroad. During FY 2007, the Department issued almost 18.4 million passports domestically and participated or assisted in the issuance of about 365,000 passports overseas.

A U.S. passport is the official U.S. government document that certifies the holder's identity and citizenship and permits travel abroad. Applications for passports require the submission of personally identifiable information (PII),⁵ such as the applicant's date and place of birth and social security number. In addition, other documentation, such as the applicant's birth or naturalization certificate, is required. The Department is responsible for maintaining the integrity of U.S. passport operations and for safeguarding the PII obtained for each passport application. PII is protected by the Privacy Act of 1974 and by other applicable regulations and guidance, such as those found in Office of Management and Budget (OMB) memoranda, Presidential Directives, and the Department's Foreign Affairs Manual (FAM). Applicable laws, directives, and guidance are summarized in Appendix F.

CA uses various systems for data entry, scanning, issuing, archiving, and querying documentation for the passport operations. These systems include the Travel Document Issuance System (TDIS), the Passport Records Imaging System Management (PRISM) database, the Passport Lookout Tracking System (PLOTS), the Management Information System (MIS), the Consular Lost and Stolen Passport (CLASP) system, and the Passport Information Electronic Records System (PIERS). The passport systems also interact with other CA systems, as well as with systems of other federal agencies and private entities (see Appendix B). However, the primary system or tool that CA uses for querying archived passport records is PIERS.⁶ CA is responsible for the data integrity, security, privacy, and accountability of the passport and/or consular records maintained in all passport systems, including PIERS. The interrelation of various passport systems is shown in Figure 1.

⁴ 22 U.S.C. § 211a.

⁵ 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.

⁶ Other tools, such as TDIS, are used to query in-process records.

SENSITIVE BUT UNCLASSIFIED

Appendix C, and the relevant laws, regulations, and guidance reviewed by OIG are listed in Appendix F.

OIG performed work at Department offices in Washington, DC, and Arlington, VA, from March 24 to May 2, 2008. This work included a walkthrough of the Washington, DC, Passport Agency and systems demonstrations of data access and extraction as appropriate. The review included interviews with and/or documents provided by officials from:

- The Bureau of Consular Affairs (CA)
 - Human Resources Division (CA/HRD)
 - Computer Systems and Technology (CA/CST)
 - CA's Directorate of Passport Services (CA/PPT)
 - CA/PPT's Office of Field Operations (CA/PPT/FO)
 - CA/PPT's Washington Passport Agency (CA/PPT/WN)
 - CA/PPT's Office of Passport Integrity and Internal Controls Program (CA/PPT/IIC)
 - CA/PPT's Office of Legal Affairs and Law Enforcement Liaison (CA/PPT/L)
 - CA/PPT's Senior Passport Operations Manager (CA/PPT/POD)
 - CA/PPT's Office of Planning and Program Support (CA/PPT/PPS)
 - CA/PPT's Office of Technical Operations (CA/PPT/TO)
- Bureau of Administration (A), including the Office of Information Programs and Services (A/ISS/ISP)
- Bureau of Information Resource Management (IRM), under the Chief Information Officer
- Bureau of Diplomatic Security (DS)
- Foreign Service Institute (FSI)

OIG also interviewed or received information from representatives from the U.S. Treasury Inspector General for Tax Administration (TIGTA), the Internal Revenue Service (IRS), and relevant operational units and the OIG of the Social Security Administration (SSA). These agencies have addressed similar concerns with the protection of PII in their programs and systems.

To perform limited testing to determine whether indications of unauthorized accesses may exist, OIG judgmentally developed, through a study approach (details and results of this study are in Appendix A), a listing of 150 high-profile names and, with CA's assistance, determined whether the records of these individuals had been accessed and, if so, by whom and how often. However, OIG did not determine whether the results of the study represented authorized or unauthorized accesses during this review. Where the results indicated the potential that an unauthorized access may have occurred because of a high volume of user accesses to the

SENSITIVE BUT UNCLASSIFIED

guidebooks, for all employees and managers. For example, the IRS guidebook includes a description of offenses; applicable penalties for first, second, and third offenses; and key factors to consider in applying the penalty.

OIG is aware that developing and implementing such guidance could be complicated because users include contract, Civil Service, Foreign Service, and union employees of the Department and other agencies, all of whom have their own set of standards, rights, and requirements. Nevertheless, OIG believes that for consistency and to prevent disparate treatment, the Department needs to determine the feasibility of developing and communicating a set of minimum disciplinary actions that can be applied to all users of passport systems. Therefore, CA/HRD should work with the Bureau of Human Resources to consider specific disciplinary guidelines that include a range of disciplinary actions and penalties to address user violations for passport systems.

Recommendation 17: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Human Resources, determine the feasibility of developing and implementing specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information. Consideration should be given to addressing all passport system users, including contractors, within the Department of State and with other agencies.

In their responses, neither CA nor HR concurred with the recommendation. In its response, CA stated:

In response to the instances of unauthorized access to the passport records of presidential candidates, CA and HR have developed procedures for administering progressive discipline for cases of unauthorized access and/or misuse of personally identifiable information contained in passport databases. HR/ER/CSD specifically advised against developing a table of penalties for progressive discipline because guidelines already exist within the Department's existing system of progressive discipline. In addition, any policy developed would not be applicable to both outside agencies and contractors as they do not fall within the jurisdiction of CA and HR for disciplinary action. For contractors, CA will coordinate with the appropriate Contracting Officer/Contracting Officer's Representative to contact the company of the person suspected or confirmed of unauthorized access to take appropriate disciplinary action. For outside agencies, CA will contact the appropriate point of contact as specified in the Memorandum of Understanding, or as otherwise directed by the federal agency, to share the passport data for appropriate disciplinary action. CA always maintains the ability to suspend access to employees, to include contractors, and federal agency employees, where it determines unauthorized access has occurred.

In its response, HR stated:

Specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information are not necessary. The Department's regulations at 3 FAM 4370 and 3 FAM 4321 set forth the guidelines for handling discipline, and these guidelines are sufficient to address misconduct related to accessing PIERS records. Similarly, the Department's regulation at 3 FAM 4377 provides the list of disciplinary offenses and penalties. The intent of the table is to serve as a general guide only, to provide a broad-range of offenses and penalties (reprimand to removal), and is not intended to provide an exhaustive list of every possible job-related offense. In practice, this table is referenced as a guide for discipline against both Civil Service and Foreign Service employees. The table includes "improper use of official authority or information" as a nature of offense that could adequately address misconduct related to accessing PIERS records. It is not necessary to add to the existing list of offenses or create a separate table. Contractors and other non-DOS employees are disciplined by their respective employers. The Department has no authority to discipline such individuals.

OIG understands the position presented by CA and HR against developing and implementing specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information. However, given the government-wide emphasis on safeguarding PII and the practices of other agencies with similar unauthorized access concerns (i.e., IRS and SSA), OIG believes that CA and HR should determine the feasibility of developing disciplinary guidelines and actions for all types of passport system users—internal and external. OIG believes that establishing and communicating disciplinary actions would also serve as a deterrent to unauthorized accesses. Further, OIG does not believe that the FAM sections cited adequately address OIG's concerns, because 3 FAM 4321 applies only to Civil Service and 3 FAM 4370 and 4377 apply only to Foreign Service personnel. In addition, CA will need to modify its MOUs with external agencies to address even minimal disciplinary actions, such as deactivating the account of a user with a suspected unauthorized access violation, while an investigation commences. In consideration of the positions presented by CA and HR, OIG has modified the recommendation.

On the basis of both responses, OIG considers this recommendation unresolved. This recommendation can be considered resolved when CA and HR agree to determine the feasibility of developing and implementing the disciplinary guidelines and the table. The recommendation can be closed when OIG receives documentation that the feasibility study has been completed.

Other Matters

During its review, OIG was also made aware of other activities that raise concerns about the safeguarding of PII in passport systems relating to both Department and non-Department users.

Required Reviews Identify Security Vulnerabilities With Passport Systems

PIERS is identified as a major system of the Department under the Federal Information Security Management Act (FISMA). As such, it is required to undergo periodic certification and accreditation²⁰ by IRM's Office of Information Assurance (IRM/IA). Access control testing is part of the certification testing performed to support the Authorization Decision that PIERS can be used or operated. According to IRM/IA officials, reviews of access controls were performed for both PIERS and PRISM. The system administrators, under the authority of the system owner (CA), review user-level access and provide the results of annual testing of selected security controls to IRM/IA for review. According to IRM/IA officials, through the certification and accreditation process, the vulnerabilities and safeguards to prevent breaches in PIERS are known. An IRM representative is on the Working Group and also participates on two of the functional areas that are addressing planned system changes and enhancements that are designed to further protect PII data contained in PIERS and other CA passport systems.

Another FISMA and OMB requirement is the conduct of the Privacy Impact Assessment (PIA),²¹ which, for PIERS, is submitted by CA to A/ISS/IPS. The representatives of A/ISS/IPS conduct a "privacy review," in which they examine the mission-related necessity of each element of collected PII as explained by the systems owner in the PIA. However, an official with A/ISS/IPS told OIG that the office is not equipped to perform a technical test of the system but tries to validate the information in the PIA to the extent possible. Ultimately, the office depends on the system owner to complete the PIA accurately. According to this official, the PIA for PIERS is currently being updated.

OIG reviewed the most recent (undated) PIA for PIERS. Regarding the controls in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access, the PIA states:

PIERS tracks and logs the activities of system users. It logs the authorized user and timestamp in which it was accessed. Training materials provided during employee orientation define the proper use and handling of privacy related data.

Regarding the question of whether other agencies share data or have access to the data in this system, the response in the PIA was "No."

The PIA information appears to contradict what OIG observed during the course of this review. While PIERS may track and log user access, it does not maintain information regarding what specific activities were conducted or why the system was accessed. Further, CA officials

²⁰ Certification and accreditation require documentation of security planning, including risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

²¹ A Privacy Impact Assessment (PIA) is a process for examining the risks and ramifications of using information technology to collect, maintain, and disseminate information in identifiable form from or about members of the public and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

SENSITIVE BUT UNCLASSIFIED

have stated to OIG that the data in PIERS is accessed by other agencies via the CCD web portal and as coordinated through Memoranda of Understanding and Memoranda of Agreement.

Recommendation 18: OIG recommends that the Bureau of Consular Affairs ensure the accuracy of its Privacy Impact Assessments (PIA) for PIERS regarding all user access (internal and external) and review the PIAs for all other passport systems to accurately reflect security controls for and risks to personally identifiable information.

In its response, CA agreed with the recommendation, stating:

CA conducts regularly scheduled PIAs on all its databases and applications to include PIERS. As a result of the incidents of unauthorized access, we are in the process of reevaluating the level of detail associated with the PIA so they can more accurately measure the Bureau's exposure to breaches of PII.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives the results of the reevaluation of the PIA for PIERS.

System-Wide Review Needed to Identify Vulnerability and Risk

OMB mandated federal agencies to review their current holdings of all PII and to ensure, to the maximum extent practicable, that such holdings are accurate, relevant, timely, and complete and reduce them to the minimum necessary for the proper performance of a documented agency function.²² These system reviews should be completed every 3 years. A/ISS/IPS officials said that they plan to work with the Department's bureaus and offices to meet this mandate, including CA's passport operations. As part of this effort, A/ISS/IPS officials indicated that they would like to undertake an end-to-end business process review that will encompass both the handling of the hard-copy passport application and its imaging and storage in the various computer systems and databases (see Appendix B). However, A/ISS/IPS officials stated that the office does not presently have the resources available to begin this task.

Officials from CA/PPT/TO also believe that an examination of the vulnerabilities and weaknesses of all passport systems should be conducted, even of those passport systems that are within the normal 3-year review cycle. The office has previously requested, but has not received, funding to begin such reviews. In addition, the Working Group is proposing that vulnerability and risk assessments be performed for all passport systems.

Given the weaknesses and data vulnerabilities identified in PIERS during this review, OIG fully agrees that such examinations of vulnerabilities and weaknesses in passport systems are warranted and necessary. Accordingly, OIG believes that the Department should make resources available to conduct the assessments as quickly as possible.

²² "Safeguarding Against and Responding to the Breach of Personally-Identifiable Information," OMB M-07-16, dated May 22, 2007.

SENSITIVE BUT UNCLASSIFIED

Recommendation 19: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Consular Affairs, conduct the necessary vulnerability and risk assessments of all passport systems and report the results of the assessments to the Bureau of Information Resource Management, Office of Information Assurance, and to OIG no later than 120 days after issuance of this report. The report of the results of the assessments should include recommendations to address any weaknesses and vulnerabilities identified, as well as a timetable for implementing corrective actions.

Both A and IRM responded to and agreed with this recommendation. CA did not respond.

In its response, A stated:

The Bureau of Administration (A) concurs with the OIG's recognition that system wide reviews are needed to identify vulnerabilities and risks in systems containing Personally Identifiable Information. As further noted in the report, the requirement to conduct Privacy Impact Assessments allows system owners to identify potential privacy risks. To this end, the A Bureau concurs with the objective that the Bureau of Consular Affairs (CA) work with both the A Bureau and the Office of Information Resource privacy reviews to ensure a comprehensive evaluation and where necessary, create mitigation strategies to address vulnerabilities. The A Bureau will coordinate its findings with the Office of Information Resource Management, which is responsible for conducting *Vulnerability and Risk Assessment*. Also, the A Bureau concurs with the statement that timely reviews and reports cannot be done without adequate resources for not only CA systems, but also other Department systems containing PII.

In its response, IRM stated:

IRM's Office of Information Assistance (IA) stands ready to assist CA in their efforts to update the vulnerability and risk assessments of their passport systems. Likewise, IA stands ready to assist A in ensuring that the update Privacy Impact Assessments are incorporated into the certification and accreditation packages of those passport systems.

On the basis of A's and IRM's responses, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the necessary vulnerability and risk assessments of the passport systems have been completed and a corrective action plan is reported to IRM/IA.

Re-disclosure of Passport Records to Third Parties

CA's policy, as stated to OIG and included in CA's MOUs with agencies that have been given access to PIERS data, is that requests by third parties for information from passport

SENSITIVE BUT UNCLASSIFIED

Based on comments received and discussions held on the draft of this report, OIG clarified the finding and recommendation for this discussion in this final report. On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has established policies and procedures addressing third party issues and has included these requirements and restrictions in all established MOUs with agencies that access PIERS data.

Memoranda of Agreement and Memoranda of Understanding With Other Federal Agencies

According to CA, about 8,000 (or 40 percent) of PIERS users work for federal agencies other than the Department, with the majority (about 7,700 users) associated with DHS. CA has an MOA or an MOU with each of these agencies that formalizes the relationships and defines the responsibilities of each of the parties. These agencies include the following:

- Department of Homeland Security
- Human Smuggling and Trafficking Center (Department of State)
- Terrorist Screening Center (Department of Justice)
- Office of Personnel Management
- Social Security Administration
- Federal Bureau of Investigation

OIG's review of two such MOUs found that although they addressed privacy concerns and access to PIERS data, there were some differences in content and the specificity of the agreements. For example, one MOA stated that the agency "shall identify in writing to Consular Affairs the specific measures taken, or expected to be taken, regarding the protection of information from unauthorized disclosure." The other MOU did not contain this requirement. Neither MOU stated that CA had the right to restrict, remove, or deny access to users found to have accessed or disclosed PIERS data inappropriately.

Several of the recommendations in this report, as well as recent initiatives by CA (especially the move to develop and implement tiered access to PIERS), will make it necessary to revise the MOAs and MOUs to address specific issues and actions. OIG believes that other agencies and entities should be held accountable and should hold their users to at least the same standards and requirements as those of Department users.

Recommendation 21: OIG recommends that the Bureau of Consular Affairs review its Memoranda of Agreement and Memoranda of Understanding with all other federal agencies and other entities to ensure that they are revised to adequately and specifically address issues related to PIERS and the passport data it contains, including the following:

- periodic verification that users and certifying authorities are in positions that merit their access to PIERS;
- annual certifications by users and certifying authorities that they have read and understand the Privacy Act and their obligation to safeguard passport records and the privacy of passport applicants;

SENSITIVE BUT UNCLASSIFIED

Abbreviations

A	Bureau of Administration
A/ISS	Office of Information Sharing Services
A/ISS/ISP	Information Programs and Services
CA	Bureau of Consular Affairs
CA/CST	Computer Systems and Technology
CA/HRD	Human Resources Division
CA/PPT	Directorate of Passport Services
CA/PPT/FO	Office of Field Operations
CA/PPT/IIC	Office of Passport Integrity and Internal Controls Program
CA/PPT/L	Office of Legal Affairs and Law Enforcement Liaison
CA/PPT/POD	Senior Passport Operations Manager
CA/PPT/PPS	Office of Planning and Program Support
CA/PPT/TO	Office of Technical Operations
CA/PPT/WN	Washington Passport Agency
CCD	Consular Consolidated Database
CLASP	Consular Lost and Stolen Passport
CRG	Data Breach Core Response Group
Department	Department of State
DHS	Department of Homeland Security
DS	Bureau of Diplomatic Security
FAM	Foreign Affairs Manual
FBI	Federal Bureau of Investigation
FISMA	Federal Information Security Management Act
FSI	Foreign Service Institute
HR	Bureau of Human Resources
IRM	Bureau of Information Resource Management
IRM/IA	Office of Information and Assurance
IRS	Internal Revenue Service
MIS	Management Information System
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PIA	Privacy Impact Assessment
PIERS	Passport Information Electronic Records System
PII	Personally Identifiable Information
PLOTS	Passport Lookout Tracking System
PPGB	Privacy Protection Governance Board
PRISM	Passport Records Imaging System Management
SSA	Social Security Administration
TDIS	Travel Document Issuance System
TIGTA	U.S. Treasury Inspector General for Tax Administration

OIG Study – Access to Passport Information of High-Profile Individuals

The Office of Inspector General (OIG) conducted a study of the passport records of 150 high-profile individuals to determine whether the unauthorized accesses to the files of three U.S. Senators in January and March 2008 were isolated instances or indications of a larger problem. The study was conducted to identify indications of potential unauthorized accesses. OIG also used the study to gain information on the controls and processes the Bureau of Consular Affairs (CA) had in place to safeguard passport records. The methodology and results of the study are discussed below.

Methodology

As discussed in the report, OIG reviewed the list of high-profile names that the Department of State included in its Monitor system and found that it was very limited in the number and types of individuals captured. For example, the list contained the names of 38 of about 127 million passport holders and excluded many other high-profile individuals, including key political figures, celebrities, and other prominent people frequently mentioned in the media.

To conduct this study, OIG developed its own list of individuals whose occupations or achievements made them newsworthy. Categories of individuals included politicians; movie, television, and media personalities; musicians; and athletes. After developing the categories, OIG used several sources to select the names. For example, OIG examined Google's 2007 and 2006 lists of most searched names and used lists developed by *Forbes* magazine (lists of top 100 celebrities and 400 richest Americans), MSN Encarta (10 Most Powerful American Women), and *Sports Illustrated* ("The Fortunate 50" highest paid athletes in 2007). OIG also selected the names of individuals who had been recently reported about in the media. After judgmentally selecting the 150 names, OIG researched the Internet to determine each individual's full legal name and date and place of birth. This level of identification allowed CA to more efficiently search for passport records for the individuals.

OIG provided the list to CA and requested detailed information on how many times, if any, the passport records of each individual had been accessed from September 2002 through March 2008. To fulfill OIG's request, CA had to take the following actions:

- search—in some cases multiple times using variations of the OIG provided-information—each individual's name to determine whether passport records existed;
- enter each individual's passport number, or numbers if they had multiple passports, into the Monitor system; and

**Laws, Directives, and Guidance
on Protecting Personally Identifiable Information**

The federal government has set forth requirements to protect personally identifiable information (PII) and to safeguard information maintained in computer systems. In addition, the Department of State and the Bureau of Consular Affairs have issued written guidance addressing access to and protection of passport records in their systems. Governing laws, directives, and guidance relating to the protection of passport data and systems are in Table 1.

Table 1. Laws, Directives, and Guidance

Federal Requirements (General)	
The Privacy Act of 1974 (as of January 3, 2005)	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)
Computer Fraud and Abuse Act 18 U.S.C. § 1030	This is a computer security law that protects computers in which there is a federal interest, such as federal computer systems. Violation of this law potentially triggers subsection (a)(2)(B), which outlaws obtaining information by unauthorized computer access. Anyone who “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains [. . .] information from any department or agency of the United States” has violated this provision and is subject to the criminal penalties described in subsection (c). It is important to note that under this provision, the mere attempt to obtain information by unauthorized computer access is a crime subject to the penalties cataloged in subsection (c). 18 U.S.C. § 1030(b). Paragraph (a)(2) is a somewhat unusual conversion statute in that it does not require any larcenous intent. The attendant penalties include the following array: <ul style="list-style-type: none">• Simple violations: not more than one year of imprisonment and/or a fine under title 18• Violations for gain or involving more than \$5000: not more than five years of imprisonment and/or a fine under title 18• Repeat offenders: not more than ten years of imprisonment and/or a fine under title 18

SENSITIVE BUT UNCLASSIFIED

<p>OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”* (May 22, 2007)</p>	<p>This Office of Management and Budget (OMB) memorandum requires agencies to:</p> <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.
<p>OMB A-130 (Revised), Management of Federal Information Resources (Transmittal Memorandum #4, 11/28/2000)</p>	<p>This circular requires agencies to:</p> <ul style="list-style-type: none">• ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information and• limit the collection of information which identifies individuals to that which is legally authorized and necessary for the proper performance of agency functions.
<p>NIST Special Publication 800-53 (Revision 2), Recommended Security Controls for Federal Information Systems (December 2007)</p>	<p>This National Institute of Standards and Technology (NIST) special publication provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government.</p> <ul style="list-style-type: none">• The organization develops, disseminates, and periodically reviews/updates a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance;• The organization, at a minimum, reviews information systems accounts annually;• The information system enforces the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks.• The organization develops, disseminates, and periodically reviews/updates a formal, documented, security awareness and training policy.

*OMB Memorandum M-07-16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information,” was developed in response to Executive Order 13402, Strengthening Federal Efforts to Protect Against Identity Theft. The President established the Identity Theft Task Force to implement the policy. This required OMB to issue data breach guidance to agencies that includes identity theft risk analysis and data breach notification requirements. In addition, agencies are required to review the use of social security numbers to eliminate, restrict, or conceal the personally identifiable information in agency business processes, systems, and paper and electronic forms.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Homeland Security Presidential Directives (HSPD)	
HSPD-1, “Organization and Operation of the Homeland Security Council,” October 29, 2001	Securing Americans from terrorist attacks requires coordination across a broad spectrum of Federal, State, and local agencies. Homeland Security Council Policy Coordination Committees shall coordinate the development and implementation of homeland security policies by multiple departments and agencies throughout the Federal government, and shall coordinate those policies with State and local government.
HSPD-7, “Critical Infrastructure Identification, Prioritization, and Protection,” December 17, 2003	This directive establishes a national policy for Federal departments and agencies to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks. This directive specifies that all Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and protection of their respective internal critical infrastructure and key resources. Consistent with the Federal Information Security Management Act of 2002, agencies will identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

Department Requirements for Protecting Passport Records	
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 review 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(a)(2))• Assistant Secretary for the Bureau of Consular Affairs (CA) develops, establishes, . . . and directs policies, procedures, and regulations relating to functions of the Bureau, including the issuance of passports and related services. (1 FAM 251.1(d))• 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(a))• Prohibiting the disclosure of records from a Privacy Act “system of records” by any method (written, oral, or electronic) unless the individual to whom the records pertain has consented, unless the disclosure falls under an exemption. (7 FAM 061(c)(3))• Requiring the Department keep a written accounting of many disclosures. (7 FAM 061(c)(4))• Prescribes civil remedies and criminal penalties for non-compliance. (7 FAM 061(c)(5))• A Department employee may not release copies of passport and citizenship records from PIERS or other sources without specific authorization from CA/PPT/ILM/R/RR, which has the responsibility for releasing such records. (7 FAM 064(d)(2)) [NOTE: The FAM has not been updated to reflect the current office symbol and name, which is CA/PPT/L/LE, Office of Legal Affairs, Law Enforcement Liaison Division.]
Notice To All Employees of Passport Services: Privacy Reminder (Bureau of Consular Affairs, March 25, 2008)	<p>This Bureau of Consular Affairs notice was issued to emphasize:</p> <ul style="list-style-type: none">• Access to passport records (including photographs and related consular records) is authorized only as required for the performance of official duties.• All personnel will be held personally responsible for complying with this requirement. Any failure to adhere to these requirements may lead to disciplinary action, including termination.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

<p>Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant Personally Identifiable Information (Bureau of Consular Affairs, April 9, 2008)</p>	<p>The Bureau of Consular Affairs (CA) Directorate of Passport Services issued this interim policy for addressing breaches of passport records and an applicant’s personally identifiable information (PII) by a user of a CA database or process that stores or accesses the information. It addresses breaches under three scenarios. These scenarios consist of breaches by government and contract employees of (1) the Directorate of Passport Services, (2) other Department bureaus, and (3) other federal government agencies. Each scenario details what incidents are to be reported, who they are to be reported to, and the timeframes for reporting them. This guidance is to be incorporated into Internal Control Standards and 7 Foreign Affairs Handbook. (See Appendix D)</p>
<p>Personally Identifiable Information Breach Response Policy (Bureau of Administration, May 1, 2008)</p> <p>NOTE: Although approved, this policy had not been issued as of May 14, 2008.</p>	<p>This is the Department’s official policy for addressing breaches concerning PII that is collected, processed, or maintained by the Department, whether it is reflected in paper records or stored and/or transmitted via Department computer systems, as well as PII stored on non-Department computer systems used by or operated on behalf of the Department. This guidance is consistent with the prescribed framework in OMB Memorandum M-07-16. This policy does not supersede or supplant the requirements imposed or other laws, such as the Privacy Act of 1974. This policy will be incorporated into the Foreign Affairs Manual. (See Appendix E)</p>

SENSITIVE BUT UNCLASSIFIED

Bureau of Administration Response



United States Department of State
Assistant Secretary for Administration
Washington, D.C. 20520

UNCLASSIFIED

MEMORANDUM

TO: OIG/AUD – Mark W. Duda

FROM: A – William H. Moser, Acting *W. Moser*

SUBJECT: Comments on Draft Report *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*
(AUD/IP-08-29)

Thank you for the opportunity to review and comment on the DRAFT report pertaining to protecting privacy information of our citizens in dealing with Passport Records. Charlene Thomas, A/ISS/IPS/PRV, is the point of contact and can be reached at (202) 663-1460.

Recommendation 19: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Consular Affairs, conduct the necessary vulnerability and risk assessments of all passport systems and report the results of the assessments to the Office of Information Resource Management, Office of Information Assurance, and to OIG no later than 120 days after issuance of this report. The report of the results of the assessments should include recommendations to address any weaknesses and vulnerabilities identified, as well as a timetable for implementing corrective actions.

Response to Recommendation 19: The Bureau of Administration (A) concurs with the OIG's recognition that system wide reviews are needed to identify vulnerabilities and risks in systems containing Personally Identifiable Information (PII). As further noted in the report, the requirement to conduct Privacy Impact Assessments (PIAs) allows system owners to identify potential privacy risks. To this end, the A Bureau concurs with the objective that the Bureau of Consular Affairs (CA) work with both the A Bureau and the Office of Information Resource

UNCLASSIFIED

Bureau of Information Resource Management Response



United States Department of State
Washington, D.C. 20520

JUN 13 2008

MEMORANDUM

TO: OIG – Mark Duda
FROM: IRM/DCIO – John Streufert *John Streufert*
SUBJECT: IRM Comments on Draft Audit Report – Review of controls and
 Notification for Access to PIERS

Recommendation 19: OIG recommends that the Bureau of Administration, in coordination with the Bureau of Consular Affairs, conduct the necessary vulnerability and risk assessments of all passport systems and report the results of the assessments to the Office of Information Resource Management, Office of Information Assurance, and to OIG no later than 120 days after issuance of this report. The report of the results of the assessments should include recommendations to address any weaknesses and vulnerabilities identified, as well as a timetable for implementing corrective actions.

IRM Response: IRM's Office of Information Assurance (IA) stands ready to assist CA in their efforts to update the vulnerability and risk assessments of their passport systems. Likewise, IA stands ready to assist A in ensuring that the updated Privacy Impact Assessments are incorporated into the certification and accreditation packages of those passport systems.