

~~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)

Report Number AUD/IP-08-29, July 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~~

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, Section 209 of the Foreign Service Act of 1980, the Arms Control and Disarmament Amendments Act of 1987, and the Department of State and Related Agencies Appropriations Act, FY 1996. It is one of a series of audit, inspection, investigative, and special reports prepared by OIG periodically as part of its oversight responsibility with respect to the Department of State and the Broadcasting Board of Governors to identify and prevent fraud, waste, abuse, and mismanagement.

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 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 cursive script, appearing to read "Mark W. Duda".

Mark W. Duda
Assistant Inspector General for Audits

Address correspondence to: U.S. Department of State, Office of Inspector General, Washington, D.C. 20522-0308

SENSITIVE BUT UNCLASSIFIED

TABLE OF CONTENTS

| | |
|---|-----|
| EXECUTIVE SUMMARY | 1 |
| BACKGROUND | 7 |
| OBJECTIVES, SCOPE, AND METHODOLOGY | 11 |
| RESULTS | 15 |
| Management Controls for PIERS User Accounts Not Adequate to Prevent Unauthorized Access | 15 |
| Detection of Unauthorized Access Unlikely | 28 |
| Department Unable to Respond Effectively to Incidents of Unauthorized Access | 34 |
| Other Matters | 43 |
| LIST OF RECOMMENDATIONS | 53 |
| ABBREVIATIONS | 59 |
| APPENDICES | |
| A. OIG Study – Access to Passport Information of High-Profile Individuals | 61 |
| B. Descriptions of Major Passport System Components | 65 |
| C. Corrective Actions by Consular Affairs in Response to Incidents of Unauthorized Access | 71 |
| D. CA Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant PII | 77 |
| E. Department’s PII Breach Response Policy | 91 |
| F. Laws, Directives, and Guidance on Protecting Personally Identifiable Information | 103 |
| G. Bureau of Consular Affairs Response | 109 |
| H. Bureau of Administration Response | 123 |
| I. Bureau of Human Resources Response | 125 |
| J. Foreign Service Institute Response | 127 |
| K. Bureau of Information Resource Management Response | 129 |

EXECUTIVE SUMMARY

In March 2008, media reports surfaced that the passport files maintained by the Department of State (Department) of three U.S. Senators, who were also presidential candidates, had been improperly accessed by Department employees and contract staff. On March 21, 2008, following the first reported breach and at the direction of the Acting Inspector General, the Office of Inspector General (OIG), Office of Audits, initiated this limited review of Bureau of Consular Affairs (CA) controls over access to passport records in the Department's Passport Information Electronic Records System (PIERS). Specifically, this review focused on determining whether the Department (1) adequately protects passport records and data contained in PIERS from unauthorized access and (2) responds effectively when incidents of unauthorized access occur.

As of April 2008, PIERS contained records on about 192 million passports for about 127 million passport holders. These records include personally identifiable information (PII), such as the applicant's name, gender, social security number, date and place of birth, and passport number. PIERS offers users the ability to query information pertaining to passports and vital records, as well as to request original copies of the associated documents. As a result, PIERS records are protected from release by the Privacy Act of 1974.¹ Unauthorized access to PIERS records may also constitute a violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030).

According to CA officials, there were about 20,500 users with active PIERS accounts as of May 2008, and about 12,200 of these users were employees or contractors of the Department. PIERS is also accessed by users at other federal departments and agencies to assist in conducting investigations, security assessments, and analyses.

OIG found many control weaknesses—including a general lack of policies, procedures, guidance, and training—relating to the prevention and detection of unauthorized access to passport and applicant information and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated. In some cases, Department officials stated that the lack of resources contrib-


¹With certain exceptions, the Privacy Act prohibits an agency's release of information in an individual's records that includes, but is not limited to, information on an individual's education; financial transactions; medical, criminal, or employment history; and name or identifying number (i.e., Social Security number).

uted to the lack of controls and to the Department's ability to assess vulnerabilities and risk. OIG has made 22 recommendations to address the control weaknesses found.

Prevention OIG found no automated or managerial mechanisms in place to provide any assurance that all PIERS users and certifying authorities could be identified or have a current need for PIERS information based on the performance of their official duties. Actual PIERS data was also used during training sessions, whereby a student could access the passport records of anyone in the system. Specifically, OIG found that the Department:

- could not readily identify the universe of all PIERS user accounts;
- was not providing adequate control or oversight of the more than 20,000 estimated PIERS user accounts it later identified to ensure that access was authorized only as required for the performance of official duties;
- did not verify that all authorized users and the more than 300 certifying authorities (who grant user access) were still in positions that merited such access and authority;
- made use of actual PIERS data for training users rather than simulated data; and
- did not implement adequate controls to prevent or detect an unauthorized access, similar to those controls in place at the Internal Revenue Service and the Social Security Administration that are used to protect large amounts of electronic PII, such as having tiered user access permissions for granting access at level needed (e.g., limited to full), blocking user access from certain records, and conducting audits of access activity logs.

Detection OIG found that the Department was ineffective in detecting possible incidents of unauthorized access because:

- the names of only a limited number of purported high-profile individuals were targeted for e-mail alerts to CA management when the records of any of these individuals were accessed. Individuals were considered to be "high-profile" if they generated significant media coverage and/or public interest or notoriety, such as entertainment and sports celebrities and politicians.

- although PIERS contains an audit trail that identifies users who access the records of any of the 127 million passport holders, this data was neither readily available nor reviewed, and except for accesses to the records of a limited number of individuals that would trigger an e-mail alert, there were no other proactive programs or provisions in place to detect access to the records of the larger universe of individuals.

- there is no mechanism in place to capture why a passport record was accessed, and there is only one individual in CA who, through a series of manual steps, tries to determine the purpose for a targeted access and whether the access appeared to be for a legitimate need based on the user's account profile before contacting the PIERS user and/or supervisor to obtain explanations for the access.
- no analysis is conducted to identify trends or indicators for excessive or suspicious user access activity, thereby rendering the magnitude of potential unauthorized access as unknown.

Response OIG found that the Department was unable to respond effectively to incidents of unauthorized access because of a number of procedural deficiencies. Specifically:

- PIERS user account data was sometimes incomplete or inaccurate, making follow-up difficult;
- a user's reasons for accessing individual records could not be readily or independently determined without ultimately contacting the user;
- no breach notification policies or procedures were in place for reporting incidents; and
- no specific guidelines for disciplinary actions against users who made an unauthorized access currently exist.

OIG did not verify instances of unauthorized access, but it did conduct a judgmentally determined study at the initiation of this review to identify the frequency with which the records for 150 high-profile individuals were accessed in PIERS between September 2002 and March 2008. Seven of the 150 selected individuals were also included in the Department's listing of a limited number of high-profile individuals. OIG's results revealed several patterns that raised serious concerns about the potential for undetected unauthorized access to passport records. For example, the passport records of one high-profile individual were accessed a total of 356 times by 77 different users. Additionally, the passport records for another high-profile individual were accessed 313 times by 54 different users. In these occurrences, a user may have accessed the records of a high-profile individual on more than one occasion or gone through the records of a high-profile individual screen-by-screen on a single occasion. OIG counted each instance of a record access separately, even if the records belonged to one high-profile individual. In both cases, the users who accessed these records were located in different regions of the country. OIG also found that some users had accessed the records of multiple high-profile individuals. For example, one user accessed the files of 38 of the 150 individuals, while another accessed 27. Users with indications of excessive and potential unauthorized accesses to passport records were referred to OIG's Office of Investigations for further review.

SENSITIVE BUT UNCLASSIFIED

OIG became aware of other activities that raise concern about the safeguarding of PII in passport systems, such as the following:

- the accuracy of the PIERS Privacy Impact Assessment regarding controls for preventing unauthorized browsing of passport data and whether data is shared with other agencies,
- the need to perform vulnerability and risk assessments and the lack of resources to do so,
- the re-disclosure² of PII to third parties and the lack of proper consent to do so,
- inconsistent agreements with other agencies to address adequate safeguarding of controls, and
- ongoing activities to transfer PIERS passport data to the Department of Homeland Security (DHS) and the development of sufficient controls to safeguard PII.

Following the publicized passport record breaches, the Department implemented a number of corrective actions, including the items noted, and has other efforts planned, as detailed in this report.

- March 24, 2008: The Working Group to Mitigate Vulnerabilities to Unauthorized Access to Passport Data (Working Group) was formed to “develop a comprehensive management plan to mitigate any unauthorized access of passport records/applicant personal data, and to develop well-defined reporting procedures should a breach occur.”
- March 25, 2008: CA issued an electronic “Notice to All Personnel With Access to Consular Records” as a reminder of the requirement for safeguarding the privacy of passport applicants and passport holders.
- April 9, 2008: The Working Group developed and issued interim guidance³ and process flowcharts that identify the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to passport records and applicant PII.
- May 1, 2008: The Bureau of Administration (A) issued the Department’s “Personally Identifiable Information Breach Response Policy,” which contains Department-wide procedures for incident reporting, response, and notification.

²CA uses the term “re-disclosure” in its Memoranda of Understanding with other agencies to refer to providing passport information to third parties.

³“Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant Personally Identifiable Information,” April 9, 2008. These guidelines are a product of the CA Working Group and are not included in the Department’s Breach Response Policy, which sets forth a Department-wide approach to address breaches concerning PII that is collected, processed, or maintained by the Department.

Management Comments and OIG Response

OIG received comments to a draft of this report from Department officials with the Bureaus of CA, A, Human Resources (HR), and Information Resource Management (IRM) and from the Foreign Service Institute (FSI). (See Appendices G through K, respectively, for the written response from each organization.) All comments received were considered, and where appropriate, OIG has revised the report and recommendations to clarify the information presented.

Of the 22 recommendations made by OIG, the Department generally agreed with 19, partially agreed with 1, and did not concur with 2. Based on the responses, OIG considers 19 recommendations resolved and three recommendations unresolved. To ensure that adequate and timely progress is achieved, OIG will conduct a follow-up compliance review of the Department's implementation of the recommendations in this report, as well as CA's process for reviewing possible unauthorized accesses by users as identified in OIG's study (see Appendix A).

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

BACKGROUND

Congress established the Department of State (Department) as the sole authority to issue passports to U.S. citizens⁴, 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)⁶. The passport systems also interact with other CA systems, as well as with systems of

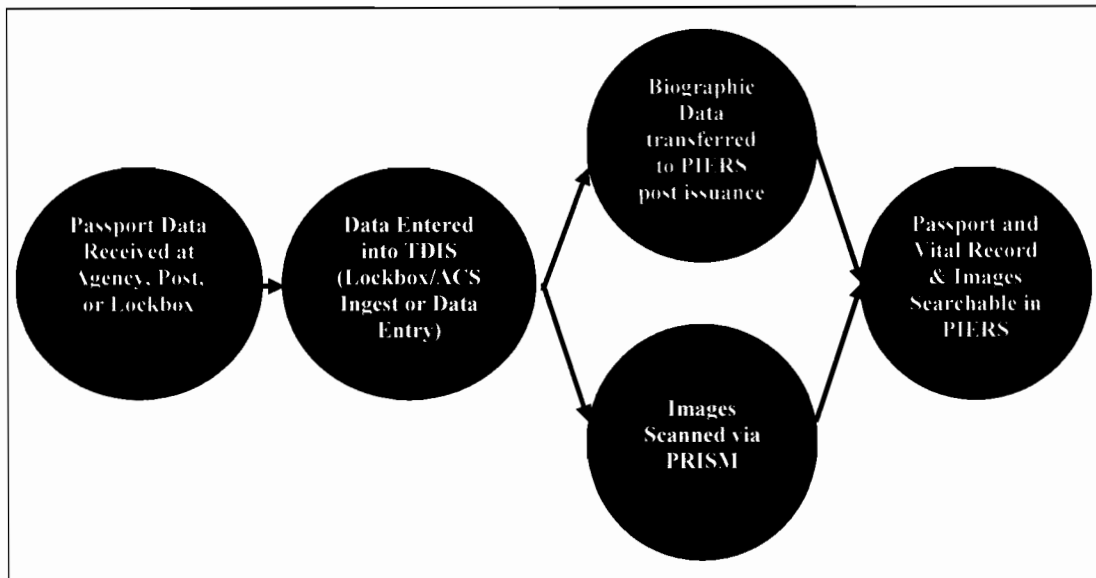
⁴ 22 U.S.C. § 211a.

⁵The 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.

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

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. 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.

Figure 1. Passport Data Input and Retrieval Process



Source: Bureau of Consular Affairs, Computer Systems and Technology (CA/CST)

Legend

TDIS: Travel Document Issuance System

PRISM: Passport Records Imaging System Management database

PIERS: Passport Information Electronics Records System

CA implemented the PIERS software application in April 1999 to improve user response time and create greater capacity and connectivity with researching passport records. PIERS offers users the ability to query information pertaining to passports and vital records, as well as to request original copies of the associated documents. Through PIERS, authorized users can view scanned images of passport applications and select supporting documentation (such as affidavits, educational records, and itineraries) for records created from 1994 to the present. In addition, PIERS contains passport applicant information, but no scanned images, for records created from about 1978 to 1993. An applicant's archived passport records are searchable in

PIERS.⁷ PIERS may be accessed by other Department users, such as CA's Overseas Citizens Services in Washington and American Citizens Services at posts worldwide, to review an individual's data for purposes such as verifying identity when a passport is lost or stolen, identifying and alerting family members when an American citizen is the victim of a disaster or dies abroad, and investigating allegations of one spouse's abduction and transport of a child outside of the United States. Users at other agencies may need access to PIERS for law enforcement and anti-terrorism purposes, such as for verifying the identity of a passport holder at a border crossing.

As of April 2008, PIERS contained records on about 192 million passports for about 127 million passport holders. Passport information is retained for the initial, renewal, and replacement passport of an applicant. These records include PII, such as the applicant's name, gender, social security number, date and place of birth, and passport number. PIERS also contains additional information, such as previous names used by the applicant, citizenship status of the applicant's parents or spouse, and scanned images of passport photos, and select supporting documentation, if applicable, submitted by the applicant. As a result, PIERS records are protected from release by the Privacy Act of 1974. Unauthorized access to PIERS records may also constitute a violation of the Computer Fraud and Abuse Act (18 U.S.C. § 1030). Under these provisions, PIERS records should be protected against any unauthorized access that could result in harm, embarrassment, or unfairness to any individual on whom information is maintained.

According to CA officials, there were about 20,500 users with active PIERS accounts as of May 2008, and about 12,200 of these users were employees or contractors of the Department. PIERS is also accessed by users at other federal agencies to assist in conducting investigations, security assessments, and analyses. These other federal entities are located across the United States and include the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and the Office of Personnel Management (OPM).

⁷Passport records are available in PIERS within 24 hours of issuance. Images are available once PRISM processing is completed, depending on the agency's schedule. Overseas issuances can take 30 or more additional days.

According to CA officials, almost all PIERS users have “read only” access.⁸ To obtain authorized access to PIERS, a user must submit a request to the certifying authority approved by CA for that organization. The certifying authority approves the request and identifies the appropriate user profile. Select users within CA can access PIERS directly, and other Department and non-Department users with an approved account for the Consular Consolidated Database (CCD) (see Appendix B) can access PIERS on-line via a web portal.

⁸A small number of CA Passport Directorate staff can edit PIERS records as required by their positions.

OBJECTIVES, SCOPE, AND METHODOLOGY

In March 2008, media reports surfaced that the passport files maintained by the Department of three U.S. Senators, who were also presidential candidates, had been improperly accessed by Department employees and contract staff. On March 21, 2008, following the first reported breach and at the direction of the Acting Inspector General, the Office of Inspector General's (OIG) Office of Audits initiated this limited review of CA's controls over access to passport records in PIERS. Specifically, this review focused on determining whether the Department (1) adequately protects passport records and data contained in PIERS from unauthorized access and (2) responds effectively when incidents of unauthorized access occur.

To make these determinations, OIG focused on PIERS, the system in which these improper accesses had occurred. For this review, OIG identified indications of weaknesses in PIERS access controls and responses to unauthorized accesses through interviews with appropriate Department officials, demonstrations, and hands-on use of PIERS and through reviews of relevant policies, procedures, and other supporting documentation. Although cognizant of the Working Group to Mitigate Vulnerabilities to Unauthorized Access to Passport Data, formed by the Department in March 2008 in response to the publicized unauthorized access incidents, OIG did not evaluate or verify the Working Group's ongoing initiatives to identify and address vulnerabilities associated with these breaches. Those initiatives are in 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 passport records of high-profile individuals, those results were provided to OIG's Office of Investigations for further review. To ensure that adequate and timely progress is achieved, OIG will conduct a follow-up compliance review of the Department's implementation of the recommendations in this report, as well as CA's process for reviewing possible unauthorized accesses by users as identified in OIG's study (see Appendix A).

This limited review was performed as a non-audit service. As such, the scope of the work performed does not constitute an audit under generally accepted government auditing standards.

On June 5, 2008, OIG provided copies of the draft of this report for comment to CA, A, HR, FSI, and IRM and met with CA officials on June 9 and 12, 2008, to discuss the findings and recommendations. The Department officials provided comments and updated OIG on the actions they planned to take to improve controls over PII in PIERS. (See Appendices G through K, respectively, for the written response from each organization.)

RESULTS

OIG found many control weaknesses — including a general lack of policies, procedures, guidance, and training — relating to the prevention and detection of unauthorized access to passport and applicant information and the subsequent response and disciplinary processes when a potential unauthorized access is substantiated. In some cases, Department officials stated that the lack of resources contributed to the lack of controls and to the Department's ability to assess vulnerabilities and risk. OIG has made 22 recommendations to address the control weaknesses identified in this report.

MANAGEMENT CONTROLS FOR PIERS USER ACCOUNTS NOT ADEQUATE TO PREVENT UNAUTHORIZED ACCESS

OIG found that the Department could not readily identify the universe of all PIERS user accounts, was not providing adequate control or oversight of the more than 20,000 PIERS user accounts it later identified to ensure that access was authorized only as required for the performance of official duties, and could not verify that all authorized users and the certifying authorities were still in positions that merited such access and authority. Actual PIERS data was also used during training sessions, whereby, as OIG observed, a student could access the passport records of anyone in the system. Further, the Department had not implemented controls to prevent or detect an unauthorized access by authorized PIERS users — similar to those controls in place at other federal agencies — for protecting large amounts of electronic PII.

Department Unable to Identify All PIERS Users

As of May 2008, CA reported to OIG that there were over 20,500 active⁹ user accounts. However CA admitted that the specific user totals it provided were only estimates because of inconsistencies in the data. When OIG initially requested information from CA on the number of PIERS users and certifying authorities and whether they worked for the Department or another federal agency, the Department could not readily produce the information. After several iterations of requesting

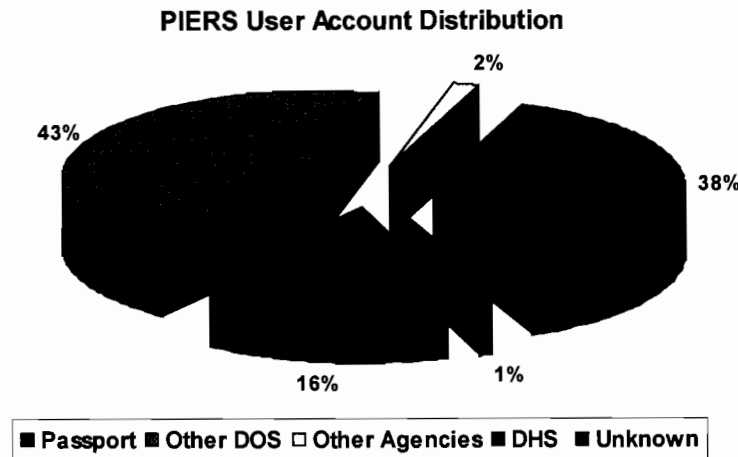
⁹A user account that has not been deactivated.

data and obtaining clarifications during a 3-week span, OIG received several sets of user account numbers. For example, with the initial results, CA could not verify the identity of and/or organization for about 1,800 active users with PIERS accounts because of missing, incomplete, and inaccurate user account data. After conducting research, CA was able to reconcile all but 170 of these users.

Based on OIG's observations, OIG determined that the difficulty CA had with providing OIG the exact universe and types of users appeared to be attributable to a combination of factors. First, the data was not readily available, and CA had to develop specific queries to generate the data. Second, in attempting to respond more precisely to OIG's request, CA used different attributes for the queries, which produced different results. Finally, the changes to user account records that occur as users are added and deleted over time cause constant changes to the universe. For example, the original query results included data for users with access to passport systems other than PIERS and produced an estimated universe of more than 23,000 user accounts. However, the results of a refined query that CA officials said represented only those users with access to PIERS as of May 1, 2008, produced an estimate of over 20,500 active PIERS accounts for about 20,350 users (some users appeared to have multiple accounts). CA was unable to further distinguish employee and contractor staff with user accounts. As shown in Figure 2, of this estimated number of users, about:

- 3,200 (16 percent) were with the CA Passport Directorate;
- 9,000 (43 percent) were with other Department bureaus, offices, or posts;
- 7,700 (38 percent) were with DHS;
- 300 (2 percent) were with other agencies; and
- 170 (1 percent) were unknown—there was not enough information to determine either the user's identity or organization.

Figure 2. PIERS User Account Distribution as of May 1, 2008



Source: OIG developed based on Bureau of Consular Affairs data.

Recommendation 1: OIG recommends that the Bureau of Consular Affairs develop a mechanism to be able to accurately, readily, and, on a recurring basis, identify the universe of all PIERS user accounts, including the organization of the user.

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

In recognition of this vulnerability, CA conducted a complete review of all PIERS user accounts in May 2008. In addition to disabling inactive accounts, we also disabled those accounts that were missing key contact information. Going forward, CA will review the PIERS user accounts on a quarterly basis (minimum) to identify any inactive accounts or those accounts with deficient contact information.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the actions described in CA's response applicable to its ability to identify all user accounts have been implemented and that CA has a process in place to review the PIERS users' accounts on at least a quarterly basis.

Authorization Needed for Performance of Official Duties Not Monitored

CA has not adequately managed user or certifying authority accounts and privileges. According to guidance contained in National Institute of Standards and Technology (NIST) Special Publication 800-53¹⁰, an organization should, at a minimum, review system accounts annually. A review includes the organization's management of its information systems accounts, including the establishment, activation, modification, review, deactivation, and removal of user accounts. As a result, the information is vulnerable to unauthorized access by users who may no longer have a valid business need for the information. According to CA officials, there have been no annual or other periodic verifications of user and certifying authority accounts and privileges performed.

User Accounts Not Periodically Validated

CA could not readily determine how many users had a valid business need for access to the system, although it noted that about 11,300 (55 percent) of the users with an active account had not accessed PIERS via the CCD web portal for 90 days or more. Specifically, 36 percent of Passport Directorate user accounts, 77 percent of other Department user accounts, 37 percent of DHS user accounts, and 66 percent of other agency and unknown user accounts had not been accessed for 90 days or more. CCD accounts that are not accessed for 90 days automatically deactivate and must be reset by a certifying authority before access is reactivated. However, according to CA officials, even if CCD access is not reset, users with access to OpenNet¹¹ are still able to access PIERS. There is currently no automatic deactivation for PIERS access based on inactivity.

¹⁰Recommended Security Controls for Federal Information Systems, NIST Special Publication 800-53, revision 2, December 2007.

¹¹OpenNet is the Department's physical internal network: the cables, switches, and routers that link the Department's offices and missions together. OpenNet is connected to the Internet via a gateway that allows certain kinds of public Internet traffic to pass onto the OpenNet.

Recommendation 2: OIG recommends that the Bureau of Consular Affairs (a) review all Department and non-Department PIERS user accounts within 60 days of the issuance of this report to identify all accounts that have been inactive for 90 days or more and accounts with incomplete or unknown identification information and (b) immediately determine whether these accounts are valid and have a current need for access. Those inactive accounts determined to have a valid need should be updated with correct and current user and access information, and those inactive accounts determined not to have a valid need should be immediately deactivated and removed to avoid reactivation.

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

In May 2008, CA reviewed all PIERS user accounts and disabled those PIERS user accounts that had not been accessed within the last 90 days. This action resulted in disabling 14,895 accounts, leaving 10,115 active accounts. Of the 10,115 active accounts, CA next disabled those accounts that were missing the name or missing key pieces of contact information (i.e. telephone number, email address, office location, office symbol). This action allowed CA to disable an additional 214 accounts. Requirements to enhance the User Manager tool in PIERS are being developed to enhance its functionality. A new tool will require certain data fields to be entered before an account can be created. Specific reporting requirements have been identified to address deficiency in user activity reporting (i.e., number of active vs. inactive accounts, active accounts by organization, etc.).

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the actions described in CA's response to review and determine the validity of inactive accounts have been implemented.

Designated Certifying Authorities Not Periodically Validated

CA does not periodically review the designated certifying authority officials to ensure that a current need exists for their continuing authority to grant system access to users. The certifying authority is responsible for all permissions granted in CCD, including PIERS. Within CA/PPT, the certifying authority is located at the passport agencies and is the Regional Director, Assistant Regional Director, or an Adjudication Supervisor. Other Department bureaus and federal agencies designate their own certifying authorities. Currently, there are about 300 active certifying authorities, and more than half of these individuals are not Department employees.

Because CA does not conduct periodic monitoring of certifying authorities, it has not maintained current contact information for each official, nor has it made a determination as to whether each official has a current need for this designation in the performance of his/her official duties (i.e., the individual may have left the organization or changed positions). As such, there may be certifying authorities with the capability to grant user rights, although they are no longer in a position that requires this authority. In addition, because of a lack of staff resources, CA has not assessed whether the certifying authority officials are performing their responsibilities appropriately.¹² Therefore, there is no assurance that a certifying authority is granting user rights that are consistent with the access needed by the user to perform his/her official duties or that the certifying authority is deactivating user accounts when there is no longer a business need for the access. Further, OIG was not provided with any evidence indicating that CA had developed or provided any training or that it had required annual certifications from these officials to ensure that they were aware of and were fulfilling their responsibilities.

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, within 120 days of the issuance of this report, identify and validate all certifying authority officials and update their contact information as needed. Those officials found to no longer have a need for this designation should be immediately deactivated and removed from CCD and PIERS user authorization capability.

In its response, CA agreed with the recommendation but required more than 60 days, as OIG had recommended in the draft of this report. CA stated:

CA has initiated a review of all certifying authority officials. CA is working with the Consular Consolidated Database (CCD) administrators to generate a list of certifying authority officials with their contact information. If there is an email address in the contact information, we will email the certifying authority and ask them to revalidate their designation. If there is no email address, we will phone them. Those with no contact information will be disabled. CA will also generate a list of all Consular System and Technology (CST) managers at all posts and request they revalidate their role as a (CST) manager. CA will need 120 days to complete this recommendation.

¹²A certifying authority should only grant access to an individual with a bona fide need, only grant rights necessary to meet that need, and deactivate a user's account when the need no longer exists.

On the basis of CA's response, OIG modified the recommendation to reflect 120 days and considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the actions described in CA's response regarding the identification and validation of certifying authority officials have been implemented.

Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with PIERS certifying authorities, verify the accuracy, completeness, and business need for all active Department and non-Department user accounts within 180 days of the issuance of this report. Those active accounts determined to have a valid need should be updated with correct and current user and access information, and those active accounts determined not to have a valid need should be immediately deactivated and disabled from reactivation.

In its response, CA agreed with the recommendation but required more than 90 days, as OIG had recommended in the draft of this report. CA stated:

Once the certifying authority list is validated, we will provide each with a list of the users they have verified and ask them to validate the users and their access information. For post, we will request that the CST manager perform this revalidation and, for passport agencies/centers, we will request that the Information Systems Security Officer (ISSO) perform this revalidation. CA will need 180 days to complete this recommendation.

On the basis of CA's response, OIG modified the recommendation to reflect 180 days and considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the actions described in CA's response regarding the validation and revalidation of user accounts have been implemented.

Recommendation 5: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures to ensure that system user accounts and certifying authority officials are reviewed on a quarterly cycle, or at least annually, in accordance with the minimum requirements contained in NIST Special Publication 800-53.

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

In the short term, CA implemented a PIERS user access request policy at all passport agencies and centers. We developed draft requirements for a system-wide user access program. The User Manager enhancements to this program will address the need to review accounts on a quarterly or annual cycle. A reporting tool for this program will give us the ability to run user account reports on ad-hoc and quarterly bases. In the long term, CA will investigate automated methodologies to further accomplish the goals of this recommendation.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the actions described in CA's response regarding the periodic review of system user accounts and verifying certifying authority officials have been implemented.

Recommendation 6: OIG recommends that the Bureau of Consular Affairs, in coordination with the Foreign Service Institute, (a) determine and provide certifying authorities with appropriate awareness guidance and/or training regarding their responsibilities, which includes verifying user information prior to granting access to PIERS and deactivating accounts as appropriate, and (b) require certifying authorities to certify annually that they are aware of and will diligently fulfill their responsibilities.

In its response, CA did not concur with the recommendation made by OIG in the draft of this report in its entirety regarding developing and providing periodic training to certifying authority officials. Specifically, CA stated:

CA/PPT is in the process of evaluating procedures for certifying authorities. We plan to implement, at a minimum, an annual signed statement from each certifying authority official affirming their understanding of their role and responsibilities in addition to verifying the validity of their user information. CA believes that the basic duties and responsibilities can be conveyed effectively in this manner, whereas creating a training class would not be cost effective. These procedures will be affirmed in revisions to the current MOUs with federal agencies we share PIERS access.

However, OIG also received a response to this recommendation from FSI. In its response, FSI stated:

FSI is currently developing a Passport Data Security distance learning course for CA which will provide initial and annual certification not just for certifying authorities, but for all PIERS users. FSI is working closely with CA to determine the best method of delivery for this course.

OIG agrees that requiring annual certifications is a positive step in achieving the intent of the recommendation. However, OIG also believes that some form of awareness guidance or training is necessary to ensure that the certifying authorities understand what they are affirming when they sign the certification. Consequently, OIG has revised the recommendation to require CA to coordinate with FSI to determine the appropriate means for providing awareness guidance or training and obtaining annual certifications.

On the basis of CA's response, OIG considers this recommendation unresolved. This recommendation can be resolved and closed when CA provides evidence that CA has coordinated with FSI to develop an appropriate awareness and certification program for all certifying authorities.

Actual Passport Data Used in PIERS Training

Students in certain consular courses at FSI¹³ accessed and used actual PIERS data as part of their training. FSI officials told OIG that actual access to PIERS had been used in training courses for several years. Two FSI officials informed OIG that students were told to access only their own passport records during the training. However, OIG was told that this was not always the case.

For example, a former student told a CA official whom OIG had interviewed that when the student trained at FSI, records of celebrities were used as examples. Also, another former student told an OIG investigator that the FSI instructor did not stress that course participants could not access PIERS files of prominent individuals after a classmate stated he/she was going to look up a celebrity's passport application. However, the FSI instructor stated to the OIG investigator that students were told not to access passport records of high-profile individuals.

Students are granted access to PIERS for the entire length of the consular courses that require such access. Although the instructors have said that they try to monitor student usage of PIERS in class, students could also access the same information outside the classroom. OIG was informed by FSI officials that students could use any of the computers provided in the study carrels or elsewhere as long as they were able to access the Department's system. According to FSI officials, student accounts are required to be deactivated at the end of each course. OIG did not confirm whether this is done.

¹³The students are primarily Department and other federal agency Civil Service, Foreign Service, or contract employees taking formal training as approved by their agencies and provided by FSI.

OIG noted in its study that nine individuals with FSI log-on accounts accessed the files of one or more high-profile names. OIG did not determine whether these individuals accessed the records while inside or outside of the FSI classroom.

OIG found no justification for allowing students at FSI to have access to actual PIERS data, because FSI currently uses simulated data for various aspects of its consular courses, such as for training on visa systems. OIG did not review training provided at any sites outside of FSI.

Recommendation 7: OIG recommends that the Bureau of Consular Affairs, (a) in coordination with the Foreign Service Institute, stop providing access to actual PIERS data for training sessions and develop an alternative approach, such as simulated PIERS data with fictional records, and (b) determine whether access to actual data is provided in other training environments, including at other agencies and contractor venues, and replace with simulated PIERS data.

In their responses, CA and FSI agreed with the recommendation. In its response, CA stated:

CA is in the process of generating a test data version of the PIERS database. We have identified commercial off the shelf software to generate the test data and are in the process of working with the A Bureau Privacy Office to identify the fields that need to be modified and/or altered. Once we generate the test data base, it will be available for all authorized OpenNet users.

In its response, FSI stated:

FSI has requested that CA/CST remove PIERS from the student profile, preventing the possibility that the students will access the system without a need to know. FSI is exploring the possibility of creating a Passport Training Database using simulated PIERS records.

On the basis of both responses, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that simulated rather than actual PIERS data is being used for all training venues.

Controls Implemented at Other Agencies Offer Examples of Good Business Practices

OIG met with and/or received information from representatives from TIGTA, IRS, and SSA — organizations also responsible for protecting large amounts of electronic PII data — to discuss their controls and found that they had established more controls to prevent and detect unauthorized access than had the Department, as well as penalties for violators. The most common of these controls are summarized in Table 1.

[REDACTED]

| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
|------------|------------|------------|------------|
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] | [REDACTED] | [REDACTED] |

[REDACTED]

The agency representatives stated that their proactive efforts help them in prosecuting users who have improperly accessed records in their systems. For example, at IRS [REDACTED]

[REDACTED] OIG believes that the collection of these controls offers examples of good business practices that CA should consider for aggressively monitoring user access to PIERS.

Recommendation 8: OIG recommends that the Bureau of Consular Affairs consider the types of controls that the Treasury Inspector General for Tax Administration, the Internal Revenue Service, and the Social Security Administration have put in place to protect electronic personally identifiable information and develop and implement a comprehensive and coordinated strategy for proactively preventing and detecting incidents of unauthorized access to PIERS.

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

The Working Group that CA convened in March 2008 met with representatives from the Internal Revenue Service, the Social Security Administration, and the Department of Veterans Affairs in April to ascertain their best practices and lessons learned related to unauthorized access of PII, their auditing systems, and reporting procedures. All three entities provided valuable information that CA is using in developing long range initiatives for monitoring, auditing, and reporting incidents of unauthorized access.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has developed and implemented a comprehensive and coordinated strategy for proactively preventing and detecting incidents of unauthorized access to PIERS.

PIERS Not Permission-Based to Limit Access

OIG found that CA had not established a system of tiered access to limit users' permissions to view only the data for which they have an authorized need to access. Currently, once a user is granted access to PIERS, all records become available and a user can view the passport application and supporting documents. However, according to CA officials, all users of the system do not need the same level of information. For example, a user with OPM may need to verify the U.S. citizenship of an applicant for a government position. This does not require a full-view image of a passport application but rather verification that a U.S. passport or Consular Report of Birth exists in the passport system. Conversely, a U.S. Customs and Border Protection user may need to verify a passport book that is questionable and need access to check more detailed identifying attributes, such as the passport number, social security number, name, or date and place of birth.

In 2007, CA began developing business requirements¹⁴ to establish access limits in PIERS so that five distinct security levels of access may be assigned to third-party agencies based on the Department's discretion. According to various CA officials, CA approved the business requirements document in April 2008 and plans to apply the access levels to all internal and external PIERS users. As currently proposed, the tiered levels will limit the information that a user receives in response to a query to PIERS. For example,

[REDACTED]

These business requirements are expected to be implemented by September 30, 2008. According to CA officials, some of the implementation issues that are not yet fully developed include the following:

- modification of the appropriate systems to reflect the assigned tier level,
- development of sufficient guidance and training to ensure that user accounts are assigned the appropriate access level,
- development of a roll-out plan (e.g., implementation all at once or phased in),
- identification of a table of minimum penalties (such as deactivation of access or temporary suspension from work) for all identified (direct hires and contractors for the Department and other federal agencies) violators who either seek or authorize unnecessary levels of access,
- development and finalization of new Memoranda of Understanding (MOU) and Memoranda of Agreement (MOA) with all external agencies that include specific guidance and requirements to ensure that agencies provide only the level of access required for each user, and
- definitions of oversight responsibilities for all appropriate Department and other agency officials to ensure that access levels are properly assigned and maintained.

Recommendation 9: OIG recommends that the Bureau of Consular Affairs develop complete PIERS business requirements to address all internal and external users of PIERS and an implementation plan that covers all aspects — such as guidance, training, verification, violations, and agreements with other agencies — before executing the new tiered-access levels.

¹⁴“PIERS Business Requirements for Restricted User Access,” Bureau of Consular Affairs, Document 1, final draft, January 28, 2008.

In its response, CA did not concur with the recommendation, stating:

CA has already completed the business requirements for tiered level access for federal agency PIERS access. The project is currently in development with a tentative completion date of Fall 2008. CA believes that the business requirements implementation plan can be efficiently done in tandem with these new levels of access. The tiered levels of access were thoroughly vetted with the Department and our outside agency partners. Waiting for completion of the implementation plan will only delay a critical mitigation mechanism to safeguard against unauthorized access. Performing these functions in tandem provides system agility that will enable CA to expand and /or contract the levels of access in real time.

OIG agrees that implementing tiered access is a critical step to safeguarding against unauthorized access to PIERS records. However, OIG found the business requirements to be ambiguous because they address only external PIERS users and not all users. While it is the intent of CA to apply the tiered-access approach to all users, the current document does not support that implementation goal. As such, OIG has modified the recommendation to clarify the actions needed. OIG believes that a comprehensive implementation plan should be developed in tandem with appropriate provisions in the MOUs with the other agencies to minimize the risk of imposing ambiguous systems requirements among agencies and loosely controlled implementation and start-up by internal and external control points.

On the basis of CA's response, OIG considers this recommendation unresolved. This recommendation can be considered resolved and closed when CA completes or clarifies its business requirements as applicable to all PIERS users and develops an implementation plan for PIERS and implements it in conjunction with the tiered-access system.

DETECTION OF UNAUTHORIZED ACCESS UNLIKELY

OIG found that unauthorized access was unlikely to be detected by the Department because the methods used were limited and ineffective; there were inadequate resources and manual processes used to follow up on potential incidents; and no analyses had been conducted to identify trends or indicators for incidents, as demonstrated in the OIG study.

Ineffective Method Used to Detect Possible Incidents of Unauthorized Access

At the time of OIG's review, the only method CA had in place to identify possible incidents of unauthorized access to about 192 million passport records in PIERS was through a separate system known as Monitor. According to CA officials, Monitor was developed on an ad hoc basis in 2005 by a group of CA managers concerned with access controls and their systems developers. It was designed to notify selected CA/PPT officials when the records of "flagged" individuals were accessed.

CA officials informed OIG, at the initiation of this review, that the names of a limited number of high-profile individuals were included in Monitor. Through this system, an e-mail alert is sent to CA management when any of the records of these individuals is accessed to initiate follow-up action to determine whether the access was authorized. The initial publicized unauthorized access to the passport records of one of the presidential candidates was detected by Monitor. Although PIERS contains an audit trail that identifies users who access the records of any of the 127 million passport holders, this data was neither readily available nor reviewed, and except for accesses to the records of a limited number of individuals that would trigger an e-mail alert, there were no other proactive programs or provisions in place to detect access to the records of the larger universe of individuals. During this review, CA officials informed OIG that CA had increased the number of high-profile individuals flagged in Monitor to over 1,000.

Through discussions with CA officials and demonstrations of Monitor, OIG learned that CA had not developed any criteria for determining which names of individuals to add or remove from Monitor. OIG was told that the number of names targeted in Monitor at the time of the publicized breaches was limited to those names that were arbitrarily added by one CA official because the individuals may have been generating media attention at the time. OIG also found that CA had not developed policies, procedures, or guidelines for investigating and determining whether access to passport records detected by Monitor was for authorized or unauthorized purposes.

Under the process in place during OIG's review, three CA officials would be notified by an e-mail alert when one of these flagged records was accessed. However, OIG learned that only one of these three individuals is responsible for responding to these Monitor alerts, thus creating a single point of failure in the notification process.

Because there is no current mechanism to capture why a passport record was accessed in PIERS, this CA official goes through a series of manual steps to determine whether the event that triggered the alert represented an authorized access, including contacting the user and the user's supervisor. However, this CA official did not always follow the same process when conducting this follow-up to an alert. Any responses received by the user or the user's supervisor regarding the reason for accessing the records were not further investigated or validated by CA officials.

Given the millions of passport records in PIERS, a more robust and effective process to monitor and detect potential unauthorized access is needed, including the appropriate resources to implement and maintain the process. CA officials do not currently have an effective method to determine which individuals should be identified for inclusion in Monitor beyond those currently included. It will also be paramount for CA to develop and implement sufficient guidance and resources to respond to a Monitor alert for both Department and non-Department users.

Recommendation 10: OIG recommends that the Bureau of Consular Affairs (CA) conduct an analysis of PIERS passport records frequently accessed by users to determine trends and excessive hits on an individual's records and to make appropriate additions to the listing of individuals contained in Monitor. From this analysis, CA should develop guidance for periodically updating the names of individuals in Monitor.

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

CA is currently drafting standard operating procedures to dictate the rules and methods to add and delete individuals from the Monitor List. We also plan to conduct coordinated PIERS user analysis with CST and Passport Services Office of Technical Operations (CA/PPT/TO). This analysis will ensure that the Monitor List contains the appropriate passport records and will implement a reporting mechanism and system alerts to identify violators who access records that are part of the Monitor List.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has completed the user analysis of PIERS and has developed and implemented the standard operating procedures for updating the Monitor List as described in its response.

Recommendation 11: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for investigating access alerts generated by Monitor and develop an independent means to identify why an access was made, such as by adding a mandatory field in PIERS to capture the reason for access.

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

In April 2008, as a result of the efforts of the Working Group that was formed to mitigate the vulnerabilities to unauthorized access, Passport Services implemented revised interim procedures for reporting and investigating potential instances of unauthorized access. Various bureaus within the Department contributed to these new procedures, to include Diplomatic Security (DS), OIG, the Office of the Legal Advisor (L), and the Bureau of Administration (A Bureau). Working with these bureaus ensured that their needs and concerns were addressed and resulted in Department-coordinated reporting and investigation procedures. In addition, CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. CA is committed to providing the necessary resources to develop a mandatory drop-down selection for entry into PIERS, requiring the user to provide a reason for their use of the database. CA believes this will act as a deterrent to unauthorized access. CA is also working with the A Bureau to build a comprehensive alert system that will better leverage technology and enhance the interim reporting procedures already in place.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has completed and implemented the actions to address the investigation and identification of unauthorized access to PIERS as described in its response.

Recommendation 12: OIG recommends that the Bureau of Consular Affairs conduct an assessment to determine the appropriate level of resources needed to effectively receive, investigate, and verify alerts for potential unauthorized access generated by Monitor.

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

Since the incidents of unauthorized access, CA has provided and will continue to provide the necessary staffing resources to the office currently responsible for overseeing the monitoring function of the PIERS database. We are currently assessing the long term needs of this office based on the short and long term initiatives being implemented.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives the results of CA's assessment of the resources needed to effectively receive, investigate, and verify alerts from Monitor.

Magnitude of Potential Unauthorized Access Unknown — A Study

OIG did not verify instances of unauthorized access, but it did conduct a judgmentally determined study at the initiation of this review to identify the frequency with which the records for 150 high-profile individuals were accessed in PIERS between September 2002 and March 2008. OIG selected the names of 150 individuals, of which seven names were also included in Monitor's listing of a limited number of high-profile individuals (the details are in Appendix A).

OIG's results revealed several patterns that raised serious concerns about the potential for undetected unauthorized access to passport records. For example, the passport records of one high-profile individual were accessed a total of 356 times by 77 different users. Additionally, the passport records for another high-profile individual were accessed 313 times by 54 different users. (In these examples, several users accessed the high-profile individuals' records multiple times. For example, one individual accessed the records of one high-profile individual 26 times during an 11-minute timeframe. Each time a record is accessed is considered a "hit."¹⁵ Therefore, the 26 accesses on one individual's passport records are considered to be 26 hits.) In both cases, the hits came from users located in different regions of the country. OIG also found that some users had accessed the records of multiple high-profile individuals. For example, one user accessed the files of 38 of the 150 individuals, while another user accessed 27. Users with an indication of excessive and potentially

¹⁵A hit could represent one of the following actions: searched for a passport, viewed a passport application, viewed supporting documentation (one hit per each page viewed), or printed an item (application or supporting documentation). Therefore, for example, if a user searched for a passport, viewed the application, and printed a copy of the application, it would register as three hits.

unauthorized access to passport records were referred to OIG's Office of Investigations for further review. The Department was unaware of these patterns because it did not have a program in place to data mine for questionable patterns, nor did it conduct audits of user access activity logs.

Recommendation 13: OIG recommends that the Bureau of Consular Affairs develop a risk-based approach to selecting PIERS users for periodic review to determine indicators of potential unauthorized access to passport records, including performing periodic audits of the existing automated activity logs available in PIERS to identify when and what records were accessed, and using data mining techniques to identify trends in user accesses to individual passport holder records.

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

In the short term, CA has implemented a formal audit program for all PIERS users within Passport Services. The audits are performed monthly by a passport agency's senior management to review both the permissions for personnel to have access to PIERS and the actual queries the employees conduct in PIERS. These audits started in April 2008 and will be done at least once a year for every employee. In addition, CA/CST is developing randomly generated lists of PIERS users for both non-Passport Services employees and PIERS users from other agencies, so random audits can also be conducted. In the long term, CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. The working group convened by CA (mentioned above) will address [REDACTED]

On the basis of discussions with CA and its written response, OIG modified this recommendation to emphasize that a risk-based approach should be taken and considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has developed and implemented the actions described in its response that will ensure a comprehensive method for user trend analysis is implemented.

DEPARTMENT UNABLE TO RESPOND EFFECTIVELY TO INCIDENTS OF UNAUTHORIZED ACCESS

Once an alert was triggered in Monitor, the Department could not respond effectively to instances of potential unauthorized access because of a number of procedural deficiencies. CA/PPT's ability to respond effectively was hampered because:

- PIERS user account data was sometimes incomplete or inaccurate, making follow-up difficult;
- a user's reasons for accessing individual records could not be readily or independently determined without ultimately contacting the user;
- no breach notification policies or procedures were in place for reporting incidents; and
- no specific guidelines for disciplinary actions to take against users who made an unauthorized access currently exist.

Lack of User Information Makes Follow-up of Alerts Difficult

CA managers could not always easily identify or contact the user and/or the user's supervisor to enable a prompt inquiry to determine whether the user had accessed the records for an authorized use or purpose. The user account information in PIERS was sometimes inaccurate, missing, or outdated. This occurred because there was no quality control over the entry of the user's identification fields.

During the OIG study, examples of data integrity problems with user information were detected, as shown in Table 2.

Table 2. PIERS User Data Discrepancies Identified in OIG's Study

| Field | Problems Noted |
|--------------|---|
| UserName | <ul style="list-style-type: none">misspelledinserted commas in the middle of a name – “doe, jo,hn”did not appear to be a valid user name – “WANGDATA” |
| OfficeSymbol | <ul style="list-style-type: none">outdatedinaccurate or unknown – “SAY”missing – field was left blank |

Source: OIG study of CA data.

These deficiencies were not isolated instances. For example, OIG found that 29 (almost 20 percent) of the 150 high-profile names were accessed by a user who was missing an office symbol in his/her account profile. Without accurate information, it was manually time consuming to identify and locate the user and/or supervisor to begin the initial contact and inquiry to determine why the passport records were accessed, especially for users outside the Department.

OIG believes that once the existing user data is reviewed and updated (see recommendations 2, 3, and 4) and policies and procedures are put in place for annual system account reviews (recommendation 5), controls must be developed and implemented to ensure a recurring data integrity process. This process could include, for example, requiring certifying authorities to verify that all user and supervisor contact information is correct and complete before approving user access, such as through the use of mandatory data entry fields.

Recommendation 14: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for quality assurance that require certifying authorities to verify user and supervisor contact information for completeness and accuracy before they grant users access to the passport systems and to confirm periodically the continuing need for the access.

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

CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. The working

group will also address the issue of managing and tracking certifying authority information. In addition, the MOU's with federal agencies will be reviewed and strengthened so the requirements for certifying authorities are detailed.

On the basis of CA's agreement with the recommendation, OIG considers this recommendation resolved, although CA did not specifically address each component of the recommendation. This recommendation can be closed when OIG receives evidence that CA has developed and implemented the policies and procedures requiring certifying authorities to verify user and supervisor contact information prior to granting access and to periodically confirm the continuing need for access to PIERS.

Reasons for Accessing Passport Records Not Readily Known

Although PIERS access activity logs capture when records were searched, viewed, and printed, the only way to determine why a file was accessed was to contact the user and/or the user's supervisor. Users were not required to indicate in PIERS why they had accessed a record, such as through choosing a task-based pull-down menu selection or entering the need for the information in a comment field. Such information would provide some basis for making an initial determination, especially if compared with other available information, such as when and where the passport was issued and the position of the employee.

Currently, the CA official responsible for following up on alerts from Monitor must complete a multi-step process to make a determination as to why a record was accessed. First, the official has to compare the PIERS data accessed with information as to when and where the passport was issued. Then a determination has to be made as to whether the user might have had a legitimate and authorized reason to access the records based on factors that included the user's position and location and when the access occurred. Ultimately, the CA official must contact the user and the user's supervisor¹⁶ to obtain an explanation about the access and to determine whether the responses received provide a valid reason for the access that occurred.

There are several potential benefits from implementing a system requirement for entering a reason for accessing a record. First, it could aid in the determination process noted above. It could serve as an additional reminder to all users and act as

¹⁶Currently, a user does not have to identify a supervisor when requesting an account log-on. As a result, the Department official has to conduct additional work to identify the correct point of contact.

a deterrent to an individual's improperly accessing a record. Additionally, it could be used in actions taken to reprimand or discipline an employee (i.e., show intent). Management could also generate statistical information to assist in work-flow analyses. Although requiring such information may add more time to the process of accessing records, OIG believes that requiring the additional information would enable CA to better determine whether the access was authorized.

Recommendation 15: OIG recommends that the Bureau of Consular Affairs (a) perform a technical and cost analysis for adding a required drop-down selection or field in PIERS to force users to identify the reason specific passport records need to be accessed and (b) identify the necessary resources to develop and implement such capability in PIERS.

In its response, CA agreed with the recommendation, referring to its response provided for recommendation 11. Specifically, CA stated:

CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. CA is committed to providing the necessary resources to develop a mandatory drop-down selection for entry into PIERS, requiring the user to provide a reason for their use of the database. CA believes this will act as a deterrent to unauthorized access. CA is also working with the A Bureau to build a comprehensive alert system that will better leverage technology and enhance the interim reporting procedures already in place.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives (a) the results of CA's technical and cost analysis for adding a drop-down selection or field in PIERS to identify the reason for accessing specific records and (b) an estimate of the resources required to develop and implement such a capability.

Policy and Guidance for Reporting PII Incidents Only Recently Established

The Assistant Secretary for Administration, as the Senior Agency Official for Privacy, is responsible for ensuring that the Department's privacy policies adhere to Privacy Act requirements and provide appropriate protection of PII in the custody of the Department. The Privacy Protection Governance Board (PPGB) was

formed to provide a focal point for the development of guidance and policies on privacy issues that impact Department operations. The PPGC established the Data Breach Core Response Group (CRG) to provide a mechanism for the Department to respond promptly and appropriately in the event of a data breach involving PII, in accordance with the guidelines contained in OMB memorandum dated September 20, 2006, "Recommendations for Identity Theft Related Data Breach Notification," and OMB Directive dated May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" (OMB Memorandum M-07-16). The CRG charter became effective on September 7, 2007.

At the time of the publicized breaches, neither CA nor the Department had implemented breach notification policies, procedures, or other criteria for reporting incidents of unauthorized access of passport records when they were detected. For example, neither OIG nor the Office of the Chief Information Officer had previously been notified of breaches of PIERS data. Specifically, there were no policies, procedures, or guidance in place that:

- defined what incidents are reportable as PII breaches;
- identified who in the Department should be notified, by whom, and when; or
- identified what documentation should be maintained for each incident.

Within CA, OIG was informed that there was an internal bureau policy of "No Surprises," which was left to individual interpretation as to what this meant and what was required. CA officials had differing opinions as to whether the three breaches of the file for one of the presidential candidates should have been reported to senior management officials. One official said that the incidents did not merit reporting beyond those officials who were alerted, despite the apparent sensitivity of this public figure. Yet another official stated that the matters should have been brought to senior management's attention. However, the CRG subsequently determined that these cases should have been treated as a breach of PII and reported to A/ISS/IPS accordingly.

According to CA officials, immediately following these breaches, a number of corrective actions were taken. Specifically:

- On March 24, 2008, the Working Group to Mitigate Vulnerabilities to Unauthorized Access to Passport Data was formed to "develop a comprehensive management plan to mitigate any unauthorized access of passport records/applicant personal data, and to develop well-defined reporting procedures should a breach occur."

- On March 25, 2008, CA issued an electronic “Notice to All Personnel With Access to Consular Records” as a reminder of the requirement for safeguarding the privacy of passport applicants and passport holders.
- In April 2008, the Working Group developed and issued interim guidance¹⁷ and process flowcharts that identify the various steps to be followed and decisions to be made in response to a potential incident of unauthorized access to passport records and applicant PII (see Appendix C).

On May 1, 2008, the Bureau of Administration issued the Department’s “Personally Identifiable Information Breach Response Policy,” which contains Department-wide procedures for incident reporting, response, and notification, which responds to the requirements of OMB Memorandum M-07-16. This policy addresses breaches of 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 (see Appendix E).

While each of these groups is to be commended on these timely actions to issue policy, procedures, and guidance, they were working independent of each other: CA to address passport-specific PII breaches and A for all types of PII breaches. For example, the notification to OIG when a breach occurs is inconsistent. Under CA guidance, CA/PPT is to notify OIG at the same time DS is notified of a passport PII breach. Under Department policy, the Diplomatic Security Computer Incident Response Team will “notify, as soon as possible, the OIG for any action that office deems appropriate” (see Appendix E). The consistency of instructions provided in these documents will be paramount for an effective PII program to address unauthorized accesses.

Recommendation 16: OIG recommends that the Bureau of Consular Affairs (CA), in coordination with the Bureau of Administration, ensure that (a) CA’s policy and the Department of State’s breach notification policies, procedures, and guidance are consistent to effectively address incidents of unauthorized access of passport records and (b) the final versions of each document are promptly incorporated into the applicable Foreign Affairs Manual and Foreign Affairs Handbook.

¹⁷“Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant Personally Identifiable Information,” April 9, 2008. These guidelines are a product of the CA Working Group and are not included in the Department’s Breach Response Policy, which sets forth a Department-wide approach to address breaches concerning PII that is collected, processed, or maintained by the Department.

In their responses, CA and A agreed with the recommendation. In its response, CA stated:

CA has and will continue to coordinate with the Bureau of Administration on all policies and procedures developed to mitigate the vulnerabilities to unauthorized access of passport records so they are in synch with A Bureau's Breach Response Policy. CA will also ensure any new policy or procedure is incorporated into the Foreign Affairs Manual and Foreign Affairs Handbook on a timely basis.

In its response, A stated:

The Bureau of Administration concurs with the recommendation that the Bureau of Consular Affairs, as well as all Department components, work in close coordination with the A Bureau to ensure consistency in all privacy policies, including incident reporting, training, and operational matters. The Department's Breach Response Policy serves as the overall guidance for addressing incidents of unauthorized access and will be incorporated in the Foreign Affairs Manual and Foreign Affairs Handbook.

On the basis of both responses, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has finalized breach notification policies, procedures, and guidance that are consistent with those of the Department and that these guidelines have been incorporated into the applicable sections of the Foreign Affairs Manual and Foreign Affairs Handbook.

No Guidance Available to Consistently Apply Disciplinary Actions

There is no guidance that details the disciplinary actions that should be taken against a user who inappropriately accesses passport records, regardless of whether the user is an employee or a contractor with CA or is external to CA or the Department. Disciplinary actions taken in CA have been left to the discretion of the supervisor and, as such, were inconsistently applied. According to CA officials, the same act of misconduct could affect CA users in different ways; that is, a PIERS user who is a contractor working in CA may get fired, while a user who is a federal employee may be counseled. Conversely, CA is not made aware of whether any disciplinary action is taken against a user who performs an unauthorized access who works in another Department organization or another federal agency.

The Department's guide¹⁸ on performance and conduct of Civil Service employees is followed by CA management when disciplining Civil Service employees who work for CA.¹⁹ This guide does not apply to contract employees, Foreign Service employees, or employees of other federal agencies. According to officials of CA/HRD, no CA employee has been reprimanded for inappropriately accessing PIERS records, and if this type of misconduct occurred in the past, it was handled at the supervisory level.

CA/HRD officials told OIG that there is no all-inclusive guidance for disciplining all types of PIERS users. For example, although CA supervisors can discipline their federal employee staffs, some of the CA employees are union members, so the supervisors must also follow union rules when applying disciplinary actions. CA management does not believe it has the authority to discipline Department employees outside CA. Further, contract supervisors, rather than CA management, discipline contract employees. CA officials said that they have limited knowledge of actions taken by officials in other Department organizations or other federal agencies for either federal or contract staff.

OIG contacted SSA and TIGTA officials to obtain information regarding how these agencies discipline their employees and contractor staff with respect to unauthorized access to PII data. Both SSA and IRS officials explained that they have developed specific guidelines that address penalty determinations in response to unauthorized access, which include reprimands, suspensions, dismissal, and prosecution. They provide this information, in the form of 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

¹⁸"Addressing Unacceptable Performance and Conduct of Civil Service Employees," U.S. Department of State, Bureau of Human Resources, Office of Employee Relations, revised January 2007.

¹⁹The first response to misconduct is to provide informal oral or written counseling to the employee to inform the employee of what was done wrong and what improvements are needed. Because CA/HRD follows progressive discipline, CA/HRD is not involved in this first phase. If the misconduct continues, formal action involving CA/HRD is taken whereby the manager writes a Letter of Reprimand, which details the misconduct, and which is then placed in the employee's Official Personnel Folder in the Bureau of Human Resources for 1 or 2 years. If the misconduct continues, the next step is suspension.

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 employ-

²⁰Certification 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.

²¹A 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.

ee 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 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

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

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.

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 databases must be directed to CA for decision and/or assistance. Agencies are not permitted to furnish or make accessible any such information to any third party (including Congress, the Government Accountability Office, courts, and the general public) without the prior written consent of CA. During the review, CA officials informed OIG of two instances in which PIERS users outside the Department had provided passport record information to a third party. In one instance, a user from another federal agency had provided hard copies of an individual's passport records to an assistant U.S. attorney (i.e., the "third party") and, in the other, to another federal entity. In both cases, a CA/PPT/L official noted that these third party disclosures were discovered only after the fact and by chance, such as when the third party contacted CA for a clearer copy of a document.

Although the Department currently has a draft MOU with DHS for review and approval, CA currently does not have an MOU in effect with DHS. Without a signed MOU in effect, DHS was not prohibited, in the two cases cited, from providing the PIERS data to third parties without CA approval. Further, OIG noted that neither the draft MOU with that agency nor two final MOUs with other agen-

cies that OIG reviewed contain any language describing what actions should be taken against users guilty of third party disclosure or by CA against the agency, such as suspending access, or any requirement for the agency to notify CA if it learns that PIERS data has been shared with third parties. It is OIG's understanding that specific restrictions in the MOUs are necessary to prohibit such disclosures by other agencies.

A CA/PPT/L official told OIG that while CA had considered establishing policies and procedures for addressing third party disclosures, none were in place and there were no established guidelines for imposing disciplinary or other actions on a passport system user or the user's agency that provides the information to a third party. The CA/PPT/L official suggested that the Department have, at a minimum, the ability to suspend the user's access to PIERS. The official also suggested that annual refresher training emphasizing this subject be required of all users, especially those users not located within CA.

Recommendation 20: OIG recommends that the Bureau of Consular Affairs (CA) (a) develop policies and procedures that address third party disclosure requirements and breaches, to include notification to CA that such a disclosure occurred and potential disciplinary and other actions that are available to CA against the individual who gave that information to the third party and the individual's agency; and (b) include these requirements and restrictions in all of its MOUs with agencies that access PIERS data.

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

CA/PPT is in the process of evaluating all of the current MOU's with the federal agencies that are granted access to the PIERS database, or are provided information from it, to ensure the proper provisions are in place to detail the procedures to follow for disclosing information to third parties and the actions to take if information is provided without State approval/consent. CA will also ensure appropriate cases are coordinated for investigation as warranted.

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;
- annual training for and responsibilities of certifying authorities, including disabling access/deactivating users' accounts immediately when access is no longer merited;
- specific guidance, criteria, and requirements to ensure that agencies provide only the level of access required by each user when tiered access to PIERS is implemented;
- oversight responsibilities for all appropriate Department and other agency officials to ensure that access levels are properly assigned and maintained;
- the agency's responsibilities for preventing, detecting, and reporting breaches and the Department's rights when it detects possible breaches made by other agency personnel; and
- minimum actions, such as deactivation of access, for identified violators who either access records improperly or authorize unnecessary levels of access.

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

CA/PPT is in the process of evaluating all of the current MOU's with the federal agencies that are granted access to the PIERS database and reaching out to the various points of contact for each MOU. CA plans to amend each MOU so each action item above is incorporated.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that CA has amended the MOUs with other agencies that have access to PIERS data.

Transfer of PIERS Passport Data to DHS Raises PII Vulnerability Concerns

CA is currently in the test phase of a project that will transfer some elements of PIERS data — the passport data page data and photographs — to DHS. This data will be transferred to DHS at the same time it is sent to PIERS when the passport book or card has completed the production process at a passport agency. DHS will store the data in its database and maintain the current status of any one passport. There is also a separate but codependent project to provide DHS with the last 10 years of archived passport data for active passports. IRM/IA officials have expressed concern as to whether the data being provided will be handled in an appropriate manner.

CA informed OIG that it is drafting the business and security requirements of these projects in an addendum to the MOA with DHS that is currently being drafted for the sharing of visa and passport records and immigration and citizenship records. Until the MOA is finalized, the draft addendum is on hold. Because the draft addendum has not been shared with OIG, OIG cannot comment on the adequacy of the controls over and the requirements for protecting this data from unauthorized and inappropriate access and/or disclosure. However, OIG does have concerns because the data will be completely out of the Department's control once it is transferred to DHS. OIG believes that the addendum must contain, at a minimum, elements to ensure that these other federal agencies and entities are held accountable for safeguarding passport records and applicants' PII.

Recommendation 22: OIG recommends that the Bureau of Consular Affairs ensure that the addendum to the Memorandum of Agreement with the Department of Homeland Security (DHS) regarding the transfer of PIERS and passport data to DHS contains, at a minimum, elements to:

- clearly identify how and by whom the data will be used;
- specify the actions to be taken against DHS should it misuse or fail to properly protect the data; and
- address specific requirements to ensure that—
 - the data is adequately protected,
 - any unauthorized and/or inappropriate access or disclosure of passport information is detected and reported to appropriate officials in CA and DHS, and
 - users who commit an unauthorized access to or inappropriate disclosure of passport data are held accountable to a minimal level that is at least comparable to CA and Department standards.

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

CA has been working extensively with DHS for years to find better ways to improve the flow of information from passport records to their personnel in the field so they can make better judgments at border crossings with regards to the legitimacy of travel documents and thus improve overall border security. Part of this initiative was to transfer appropriate passport record data directly to DHS. Based on the incidents of unauthorized access, CA is re-assessing the proposed procedures to ensure the requirements listed above are part of the MOU and day to day processes.

On the basis of CA's response, OIG considers this recommendation resolved. This recommendation can be closed when OIG receives evidence that the addendum to the MOU with DHS contains appropriate language and requirements for protecting PIERS data that is transferred to DHS.

LIST OF RECOMMENDATIONS

Recommendation 1: OIG recommends that the Bureau of Consular Affairs develop a mechanism to be able to accurately, readily, and, on a recurring basis, identify the universe of all PIERS user accounts, including the organization of the user.

Recommendation 2: OIG recommends that the Bureau of Consular Affairs (a) review all Department and non-Department PIERS user accounts within 60 days of the issuance of this report to identify all accounts that have been inactive for 90 days or more and accounts with incomplete or unknown identification information and (b) immediately determine whether these accounts are valid and have a current need for access. Those inactive accounts determined to have a valid need should be updated with correct and current user and access information, and those accounts determined not to have a valid need should be immediately deactivated and removed to avoid reactivation.

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, within 120 days of the issuance of this report, identify and validate all certifying authority officials and update their contact information as needed. Those officials found to no longer have a need for this designation should be immediately deactivated and removed from CCD and PIERS user authorization capability.

Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with PIERS certifying authorities, verify the accuracy, completeness, and business need for all active Department and non-Department user accounts within 180 days of the issuance of this report. Those active accounts determined to have a valid need should be updated with correct and current user and access information, and those active accounts determined not to have a valid need should be immediately deactivated and disabled from reactivation.

Recommendation 5: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures to ensure that system user accounts and certifying authority officials are reviewed on a quarterly cycle, or at least annually, in accordance with the minimum requirements contained in NIST Special Publication 800-53.

Recommendation 6: OIG recommends that the Bureau of Consular Affairs, in coordination with the Foreign Service Institute, (a) determine and provide certifying authorities with adequate guidance and/or training regarding their responsibilities, which includes verifying user information prior to granting access to PIERS and deactivating accounts as appropriate, and (b) require certifying authorities to certify annually that they are aware of and will diligently fulfill their responsibilities.

Recommendation 7: OIG recommends that the Bureau of Consular Affairs, (a) in coordination with the Foreign Service Institute, stop providing access to actual PIERS data for training sessions and develop an alternative approach, such as simulated PIERS data with fictional records, and (b) determine whether access to actual data is provided in other training environments, including at other agencies and contractor venues, and replace with simulated PIERS data.

Recommendation 8: OIG recommends that the Bureau of Consular Affairs consider the types of controls that the Treasury Inspector General for Tax Administration, the Internal Revenue Service, and the Social Security Administration have put in place to protect electronic personally identifiable information and develop and implement a comprehensive and coordinated strategy for proactively preventing and detecting incidents of unauthorized access to PIERS.

Recommendation 9: OIG recommends that the Bureau of Consular Affairs develop complete PIERS business requirements to address all internal and external users of PIERS and an implementation plan that covers all aspects—such as guidance, training, verification, violations, and agreements with other agencies—before executing the new tiered-access levels.

Recommendation 10: OIG recommends that the Bureau of Consular Affairs (CA) conduct an analysis of PIERS passport records frequently accessed by users to determine trends and excessive hits on an individual's records and to make appropriate additions to the listing of individuals contained in Monitor. From this analysis, CA should develop guidance for periodically updating the names of individuals in Monitor.

Recommendation 11: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for investigating access alerts generated by Monitor and develop an independent means to identify why an access was made, such as by adding a mandatory field in PIERS to capture the reason for access.

Recommendation 12: OIG recommends that the Bureau of Consular Affairs conduct an assessment to determine the appropriate level of resources needed to effectively receive, investigate, and verify alerts for potential unauthorized access generated by Monitor.

Recommendation 13: OIG recommends that the Bureau of Consular Affairs develop a risk-based approach to selecting PIERS users for periodic review to determine indicators of potential unauthorized access to passport records, including performing periodic audits of the existing automated activity logs available in PIERS to identify when and what records were accessed, and using data mining techniques to identify trends in user accesses to individual passport holder records.

Recommendation 14: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for quality assurance that require certifying authorities to verify user and supervisor contact information for completeness and accuracy before they grant users access to the passport systems and to confirm periodically the continuing need for the access.

Recommendation 15: OIG recommends that the Bureau of Consular Affairs (a) perform a technical and cost analysis for adding a required drop-down selection or field in PIERS to force users to identify the reason specific passport records need to be accessed and (b) identify the necessary resources to develop and implement such capability in PIERS.

Recommendation 16: OIG recommends that the Bureau of Consular Affairs (CA), in coordination with the Bureau of Administration, ensure that (a) CA's policy and the Department of State's breach notification policies, procedures, and guidance are consistent to effectively address incidents of unauthorized access of passport records and (b) the final versions of each document are promptly incorporated into the applicable Foreign Affairs Manual and Foreign Affairs Handbook.

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.

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.

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.

Recommendation 20: OIG recommends that the Bureau of Consular Affairs (CA) (a) develop policies and procedures that address third-party disclosure requirements and breaches, to include notification to CA that such a disclosure occurred and potential disciplinary and other actions that are available to CA against the individual who gave that information to the third party and the individual's agency, and (b) include these requirements and restrictions in all of its MOUs with agencies that access PIERS data.

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;
- annual training for and responsibilities of certifying authorities, including disabling access/deactivating users' accounts immediately when access is no longer merited;
- specific guidance, criteria, and requirements to ensure that agencies provide only the level of access required by each user when tiered access to PIERS is implemented;

- oversight responsibilities for all appropriate Department and other agency officials to ensure that access levels are properly assigned and maintained;
- the agency's responsibilities for preventing, detecting, and reporting breaches and the Department's rights when the Department detects possible breaches made by other agency personnel; and
- minimum actions, such as deactivation of access, for identified violators who either access records improperly or authorize unnecessary levels of access.

Recommendation 22: OIG recommends that the Bureau of Consular Affairs ensure that the addendum to the Memorandum of Agreement with the Department of Homeland Security (DHS) regarding the transfer of PIERS and passport data to DHS contains, at a minimum, elements to:

- clearly identify how and by whom the data will be used;
- specify the actions to be taken against DHS should it misuse or fail to properly protect the data; and
- address specific requirements to ensure that—
 - o the data is adequately protected,
 - o any unauthorized and/or inappropriate access or disclosure of passport information is detected and reported to appropriate officials in CA and DHS, and
 - o users who commit an unauthorized access to or inappropriate disclosure of passport data are held accountable to a minimal level that is at least comparable to CA and Department standards.

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**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 |

SENSITIVE BUT UNCLASSIFIED

| | |
|--------|--|
| 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 |

SENSITIVE BUT UNCLASSIFIED

APPENDIX A

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
- query the Monitor system for each passport number — only 10 "hits"²³ per record could be viewed and printed at a time.

OIG received the results of this research in hard-copy form on April 4, 2008, and compiled the information manually. This involved reviewing the results of each individual to determine whether and how many times the individual's records had been accessed (hit). After OIG issued its draft report and held subsequent discussions with CA officials, on June 18, 2008, CA provided an electronic spreadsheet containing different results. While the April data was produced by Monitor's standard query of PIERS, the June data was extracted from PIERS using a query created specifically for this purpose. Although OIG did not attempt to verify the reliability of either set of data, OIG noted, when it compared both sets of data, that there were several omissions in the April data. For example, the OIG found records in the June results that should have been included in the April results. Therefore, OIG used the June data and updated the analysis and results for the final report.

Results

Of the 150 names included in the study, OIG found that the records of 127 individuals, or 85 percent, had been accessed at least one time. The query results showed a total of 4,148 hits to the passport information for these individuals. OIG made no determination as to whether the hits, as shown in Table 1, represented authorized or unauthorized access.²⁴

²³A hit could represent one of the following actions: searched for a passport, viewed a passport application, viewed supporting documentation (one hit per each page viewed), or printed an item (application or supporting documentation). Therefore, for example, if a user searched for a passport, viewed the application, and printed a copy of the application, it would register as three "hits."

²⁴As discussed in the Section "Determining Incidents of Unauthorized Access" in the report, making a determination as to whether an access is authorized or unauthorized involves the examination of many different factors, including contacting the individual for justification as to why the file was accessed.

Table 1. Access to PIERS Passport Files

| Number of hits to Passport Files | Number of Individuals on the 150-name High-Profile List |
|----------------------------------|---|
| 0 | 23 |
| 1-25 | 85 |
| 26-50 | 15 |
| 51-75 | 15 |
| 76-100 | 3 |
| 101 or more | 9 |

Source: OIG analysis based on CA data provided June 18, 2008.

Although an 85 percent hit rate appears to be excessive, the Department currently lacks criteria to determine whether this is actually an inordinately high rate.

OIG's limited analysis of the hits to the high-profile names also showed several questionable patterns. For example, one high-profile individual's records were hit a total of 356 times by 77 different users between 2003 and 2008. Additionally, another high-profile individual's records were hit 313 times by 54 different users between 2003 and 2008. In these occurrences, a user may have accessed a high-profile individual's records on more than one occasion or gone through a high-profile individual's records screen-by-screen on a single occasion. OIG counted each instance of a record access separately, even if the records belonged to one high-profile individual. In both cases, the users who accessed these records were located in different regions of the country, as well as overseas.²⁵

Some users accessed many high-profile names. For example, one user accessed 27 high-profile names for 217 hits, another user accessed 38 high-profile names for 146 hits, and a third user accessed 24 high-profile names for 97 hits.

OIG found that the records of 12 high-profile individuals were viewed by users granted access through training at the Foreign Service Institute. (See Section "Actual Passport Data Used in PIERS Training" in the report.)

²⁵This was determined from the office symbol of the viewer captured in the Passport Information Electronic Records System report.

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

APPENDIX B

Descriptions of Major Passport System Components

Consular Consolidated Database (CCD)

The Consular Consolidated Database, or CCD, is the database in the Washington, DC, area that holds all of the current and archived data from all of the Consular Affairs post databases around the world, and it consists of several interconnected database, web, and other servers in multiple locations. The CCD also provides access to passport data in TDIS, PLOTS, and PIERS. In addition, other data is integrated into the CCD, e.g., the “Master Death Database,” from the Social Security Administration. The CCD supports query and reporting requirements, data entry requirements, as well as the full recovery of post databases. This also includes CCDI and CCDR—both are web portals to the OSIS²⁶ network.

Data in the CCD is generally presented to users via parameter driven reports which can be selected from a menu on the left side of the screen. The various CCD services and reports are divided into sections based on CA functions, such as immigrant visas, nonimmigrant visas, and other areas such as Administrative. To access the majority of the CCD services and reports, a user will require a CCD account.

The CCD, CCDR, and CCDI are accessed via a web browser, such as Internet Explorer, which is on all Department desktop computers.

[REDACTED]

Users logged on to the Department's OpenNet access the Public page of the CCD at <https://cadata.ca.state.gov>. You do not need a CCD account to access the Public page, but it contains limited reports (see the menu under the Logon box). Department users who are not connected to the Department's OpenNet but do have accounts on OSIS can connect to the CCDR by logging on to OSIS then browsing to: <https://ccdi.state.osis.gov/ccdr.html>.

Non-Department users who are not connected to the Department's OpenNet but have accounts on OSIS can connect to the CCDI by logging on to OSIS and then browsing to: <https://ccdi.state.osis.gov/ccdi.html>. The CCDI has a different start page than the CCD or CCDR. Support is the only option available on the CCDI public page. There are no public reports on the CCDI.

Consular Lost and Stolen Passport (CLASP) Database

CLASP is PPT's system for recording Lost and Stolen passports and reporting those passports to U.S. Customs. Records are entered into CLASP from TDIS, ACS and the CLASP Unit's web based CLASP system.

Consular Lookout and Support System (CLASS)

CLASS is a part of PPT's Namecheck system. It scores names based on multiple algorithms and returns the highest ranking "hits" to the Passport Specialist. CLASS is a centralized system with both the database and name-search software residing.

Management Information System (MIS)

MIS is a reporting application used to parallel query multiple databases for passport production, labor and staffing data to produce various management reports.

Passport Information Electronic Records Systems (PIERS)

The Passport Information Electronic Records System is a software application that provides the ability to search, view, create, and modify Passport Records and Vital Records. Users can request PIERS Documents and specify priorities and delivery instructions for these documents. In addition, users can view related information from the Passport Records Imaging System Management (PRISM) database.

Passport Lookout Tracking System (PLOTS)

The Passport Lookout Tracking System is a software program that provides an intranet-based system to manage all passport lookout files. The PLOTS web interface allows authorized users in various locations to access a central case record file and recall digital records. The central repository is the PLOTS Case Archive where all case information is maintained.

Passport Records Imaging System Management (PRISM) database

PRISM is a digital imaging system used on-site at passport agencies that scans and stores information in an easily retrievable format. The primary purpose of PRISM is to scan passport applications quickly, efficiently, and reliably and store these records for immediate access from any PC terminal authorized to recall the record.

Travel Document Issuance System (TDIS)

The Travel Document Issuance System (TDIS) is used domestically to manage the entirety of the passport issuance process from application receipt and payment through data entry, adjudication, printing and quality control.

Brief description of system interaction content by number:

- (1) External Agencies → CLASS: Various types of lookouts (e.g. deadbeat parents, outstanding warrants, etc.)
- (2) CLASP → Interpol: Lost and stolen passport data
- (3) CLASP → DHS: Lost and stolen passport data
- (4) CLASP ↔ CLASS: Lookout query/response
- (5) PLOTS → CLASP: Lost and stolen passport query/response
- (6) TDIS ↔ CLASS: Lookout and namecheck query/response
- (7) CLASP ↔ IPDB: In process passport application query/response
- (8) PLOTS ↔ CLASS: Manage lookouts and lookout query/response
- (9) PIERS → IPDB: Removes entries when passport applications are no longer in process
- (10) TDIS ↔ CLASP: Lost and stolen passport query/response
- (11) CLASP ↔ PIERS: Issued passport application data query/response
- (12) PLOTS ↔ IPDB: In process passport application query/response
- (13) TDIS ↔ IPDB: In process passport application query/response
- (14) PLOTS → IMS (DS): Refer fraud cases to Diplomatic Security for further investigation and review
- (15) PLOTS ↔ PRISM: Passport application or other digitized record query/response
- (16) PLOTS ↔ TDIS: Passport application data query/response (response can be imported into PLOTS case)
- (17) MIS ↔ PLOTS: Small subset of fraud case data query/response
- (18) PLOTS ↔ PIERS: Issued passport application data query/response
- (19) TDIS → PIERS: In process and issued passport application data
- (20) TDIS ↔ PIERS: Issued passport application data and MIV query/response
- (21) PIERS ↔ PRISM: Update image/passport application index and image query/response
- (22) TDIS → MIS: Summarized application data for applicable MIS reports
- (23) TDIS ↔ PRISM: Passport application index and image query/response
- (24) TDIS (Agency) → TDIS (PCD): All data is replicated approximately every 3-5 minutes
- (25) Citi → TDIS: Lockbox application data
- (26) TDIS ↔ SSA: Validate applicant data query/response
- (27) TDIS → OPSS: Subset of application data and application status
- (28) TDIS Inquiry ↔ TDIS: Application data query/response
- (29) TRIP ↔ TDIS: Subset of application data and application status query/response
- (30) TDIS → USPS: Mailing manifest data

SENSITIVE BUT UNCLASSIFIED

- (31) TDIS ↔ SDS (IRM): Validate and encode chip in ePassport book query/response
- (32) GPO → TDIS: Shipment inventory data
- (33) PRISM (Agency) → PRISM (PCD): All data is replicated approximately every 3-5 minutes

SENSITIVE BUT UNCLASSIFIED

APPENDIX C

Corrective Actions by Consular Affairs in Response to Incidents of Unauthorized Access

To respond to the deficiencies in safeguarding passport information that surfaced in the media in March 2008, the Bureau of Consular Affairs (CA) formed the Working Group to Mitigate Vulnerabilities to Unauthorized Access to Passport Data. The Working Group was formed “to develop a comprehensive management plan to mitigate any unauthorized access of passport records/applicant personal data and develop well-defined reporting procedures should a violation occur.” The group²⁷ was to “provide equal and effective safeguards to all records of passport applicants” and “[develop] additional levels of access to . . . PIERS database.”

During the course of the Office of Inspector General’s (OIG) review, OIG’s Office of Audits staff met with various members of the Working Group. OIG was kept aware of what the Working Group was doing, and the Working Group was aware of OIG’s efforts. However, OIG did not evaluate or verify the Group’s ongoing initiatives to identify and address their systems’ vulnerabilities.

On April 28, 2008, the Acting Director of the Directorate of Passport Services formally informed OIG of corrective actions taken as a result of the Working Group’s proposals, as shown on pages 72 to 75 of this appendix. The Working Group continues to meet and is developing other proposals.

²⁷The Working Group comprises 49 individuals who represent various Department bureaus, including CA, DS, A, and L.



United States Department of State

Washington, D.C. 20520

~~SENSITIVE BUT UNCLASSIFIED~~

APR 8 2008

**INFORMATION MEMO FOR ASSISTANT INSPECTOR
GENERAL DUA - OIG**

FROM: CA/PPT Lawrence R. Bacr, Acting 

SUBJECT: Corrective Actions by Consular Affairs in Response to Incidents of
Unauthorized Access

Since the incidents of unauthorized access to the passport records of the presidential candidates came to the attention of senior management in Consular Affairs (CA) on March 20, 2008, CA has implemented a number of corrective actions and new initiatives. With these new actions and initiatives, we intend to severely mitigate and eliminate all vulnerabilities these recent breaches have revealed concerning the unauthorized access of personally identifiable information contained in CA records. Our ultimate goal is to provide equal and effective safeguards to all records of passport applicants. Attached is a list of corrective actions that have been completed or initiated.

CA stands committed to protect the privacy of passport applicants through these many initiatives. I look forward to seeing your findings and recommendations on this important issue.

Attachment:

Corrective Actions Taken By CA in Response to Incidents of Unauthorized
Access

**Corrective Actions Taken by Consular Affairs in Response to
Unauthorized Access**

On March 21st, we found that a passport contract employee was fired for improperly looking at the passport records of Senator Barack Obama. Two other contract employees were also fired after accessing the senator's records without authorization.

Subsequently, the following corrective actions have been taken:

- PPT DAS sent an e-mail to all domestic consular employees (both government and contract) reminding them of the requirement for safeguarding the privacy of passport applicants and passport systems, and the possible disciplinary actions for instances of unauthorized access.
- All PPT Regional Directors were instructed to have meetings with all employees to emphasize the importance of complying with the Privacy Act. All PPT agencies and centers held these meetings with their employees.
- PPT modified initial e-mail notification sent to users that access passport records on the Monitor List. This notification was modified to now include the PPT DAS, Managing Director, and all Office Directors.
- Effective March 23rd, all PPT employees, both contractor and direct hire government employees, were required to sign a document stating that they read and understood the requirements of the Privacy Act and their obligation to safeguard passport records and the privacy of passport applicants. All employees now on duty (both contractor and direct hire government) have read and signed the statement.
- On March 25th, a Department Notice was sent out to all personnel reminding anyone with access to CA records of the requirement for safeguarding the privacy of passport applicants and passport holders.
- On March 26, the Passport Operations Manager directed the Regional Directors of all Passport Agencies and Centers to disable access to the system for users who no longer have an official need to access it.

SENSITIVE BUT UNCLASSIFIED

- On March 24, a Working Group was formed to develop a comprehensive management plan to mitigate any unauthorized access of passport records/applicant personal data, and to develop well-defined reporting procedures should a breach occur. To date, the Working Group, co-chaired by Barry Conway (CA/PPT/IIC) and Gail Neelon (CA/PPT/L), has met four times and has directed and managed the completion of the following tasks:
 - CA formed a sub-working group to develop standardized, Department-wide disciplinary guidelines for incidents of unauthorized access.
 - CA input of Additional Names on the PIERS Monitor List – Over 1,000 individuals, including the First Family, presidential candidates and spouses, Vice President and family, current members of Congress, Cabinet members, Supreme Court Justices, state governors, former presidents, select former and members of Congress were entered into the Monitor List.
 - The checklist of questions sent via e-mail to an individual that accesses PIERS record on this Monitor list was modified to expand the capture of information needed to determine whether a breach of PPT records has occurred.
 - The criterion was clarified for involving Human Resource Division (HRD), Office of the Inspector General (OIG) and Diplomatic Security (DS) when a potential and confirmed breach of PPT records occurs.
 - The criterion was also clarified for involving A Bureau Privacy Office, Diplomatic Security-Computer Incident Response Team (DS-CIRT), and United States Computer Emergency Readiness Team (US-CERT) when a potential and confirmed breach of PPT records occurs.
 - Additional quality control testing of the Monitor List program was conducted to ensure the reliability of the program with the increased number of names.
 - CA developed and implemented revised reporting procedures and standard operating procedures (SOP) for all incidents of unauthorized access. These new procedures were put into effect on April 10th.
 - On April 17-18, CA/CST sent e-mails to all Passport Agency Information Systems Security Officers (ISSOs) and post systems administrators notifying them of requirements to limit user access and monitor use of PIERS.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

- o CA developed and mandated an interim program of random PIERS audit inquiries be completed by all PPT agencies, centers, and HQ. This program was initiated on April 18th.
- o The initial pop-up after the log-in screen for entry into the PIERS database was modified. Additional language was added, with key words and phrases bolded and highlighted in red to emphasize that the database should only be used for official business. Penalties for unauthorized access are also delineated, advising the user that the system is being actively monitored.
- o Met with other federal agencies to gather their lessons learned and best practices for protecting the personally identifiable information of their stakeholders. Meetings occurred with the SSA on April 23rd, with the IRS on April 25th, and a meeting is scheduled with VA on April 30th.
- o Updated to Passport's National Training Program for new passport specialists to enhance the existing the privacy and internal controls module already in place.

SENSITIVE BUT UNCLASSIFIED

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

APPENDIX D

CA Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant PII



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

April 9, 2008

UNCLASSIFIED
MEMORANDUM

TO: Regional Directors, Assistant Regional Directors, and Headquarters Office Directors

FROM: CA/PPT/MD – Florence Fultz, Acting *DF*

SUBJECT: Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant Personally Identifiable Information

Attached are the reporting guidelines for Passport Services management to follow in the event you determine that unauthorized access to passport records/an applicant's personally identifiable information (PII) has been performed by a user of a CA database or process that stores or accesses the information. Access to passport records (including photographs and related consular records) is authorized only as required for the performance of official duties. Any access by personnel outside of their official duties must be reported/addressed immediately by the supervisors/management of the individual who accessed the information. The incident(s) should be reported as outlined in the attached guidance and in the Department's Breach Response Policy (to be published shortly).

These guidelines must be followed so that actions can be taken immediately to mitigate the potential misuse of an applicant's personal information. Please ensure the guidelines are disseminated to your staff as soon as possible. These guidelines will be incorporated into the Internal Controls Standards and the 7 Foreign Affairs Handbook (FAH).

Please note that these guidelines are being issued on an interim basis. I encourage your feedback and suggestions to continually improve the process. In the short and long term, PPT will continue to modify these procedures and take advantage of any technology to make the process more efficient.

SENSITIVE BUT UNCLASSIFIED

UNCLASSIFIED

2

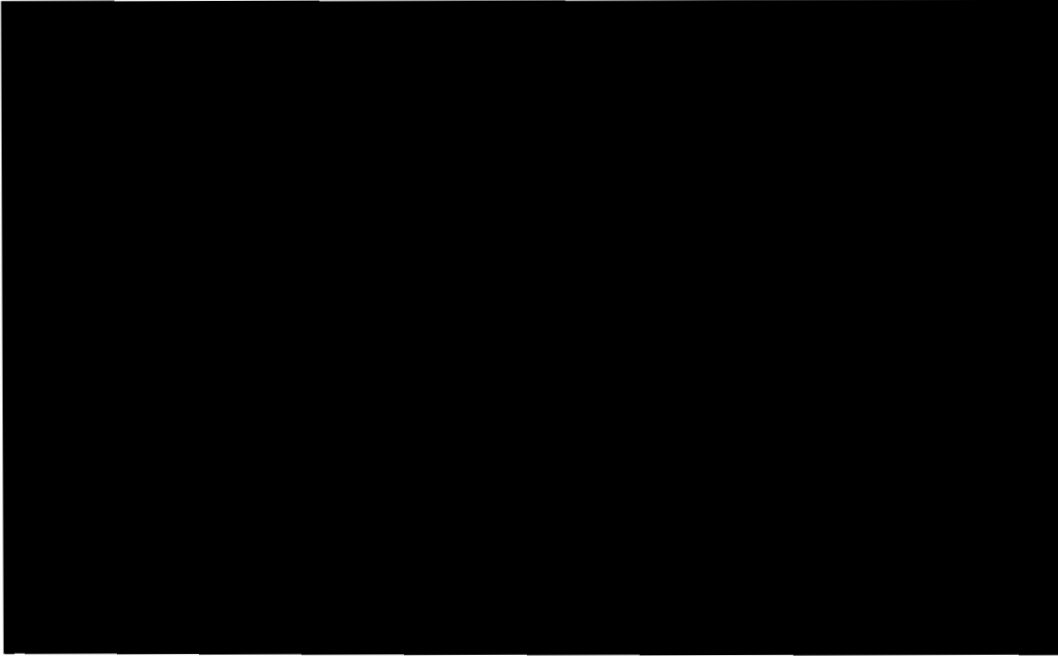
Attachment:

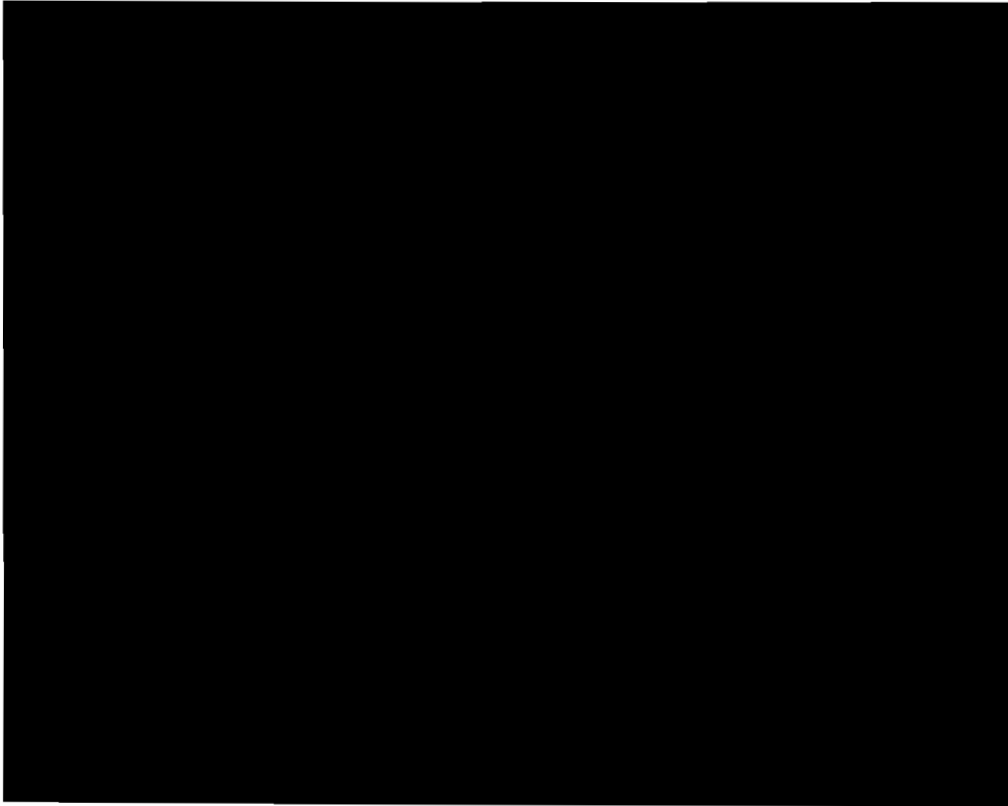
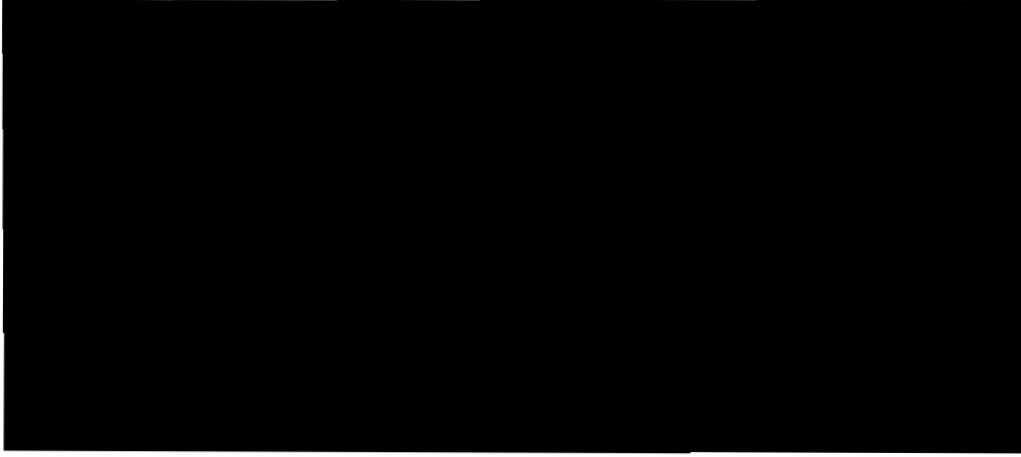
Reporting Guidelines for Incidents of Unauthorized Access to Passport
Records/Applicant Personally Identifiable Information

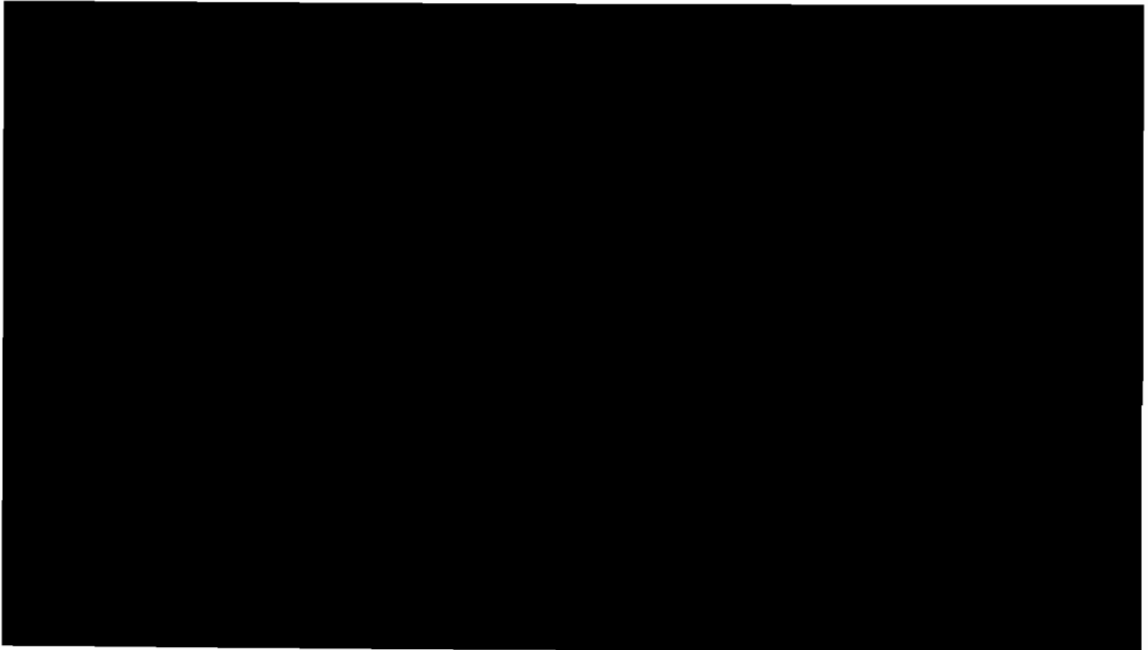
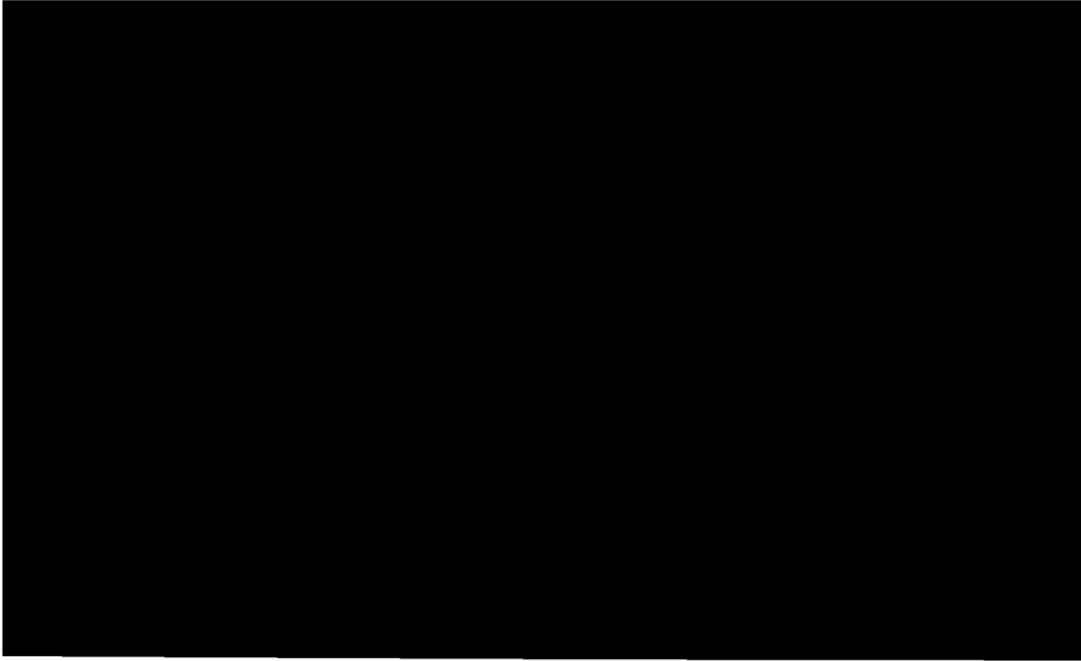
CC: A/ISS/IPS/PRV: CThomas
DS/SI: FWilkens
L-CA: GBrancato
L-M: JWeinberg
L: JBorek
FSI/SAIT: JScottNorris
CA/PPT/CM: SCowlishaw
CA/PPT/IA: RMHolly

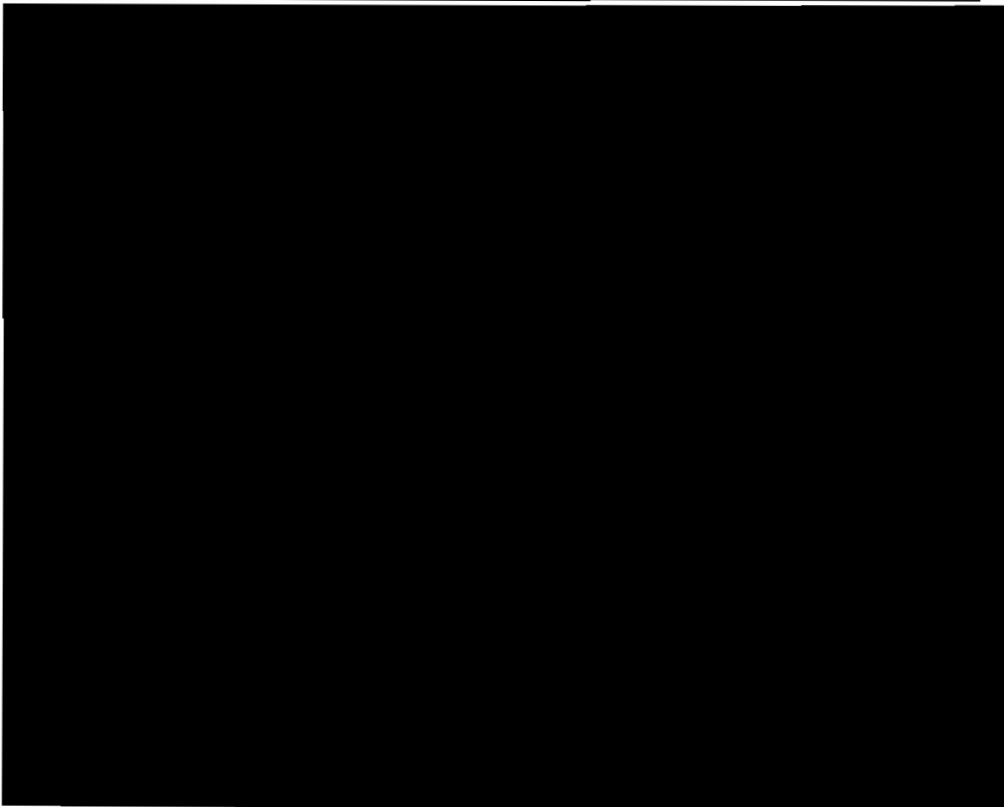
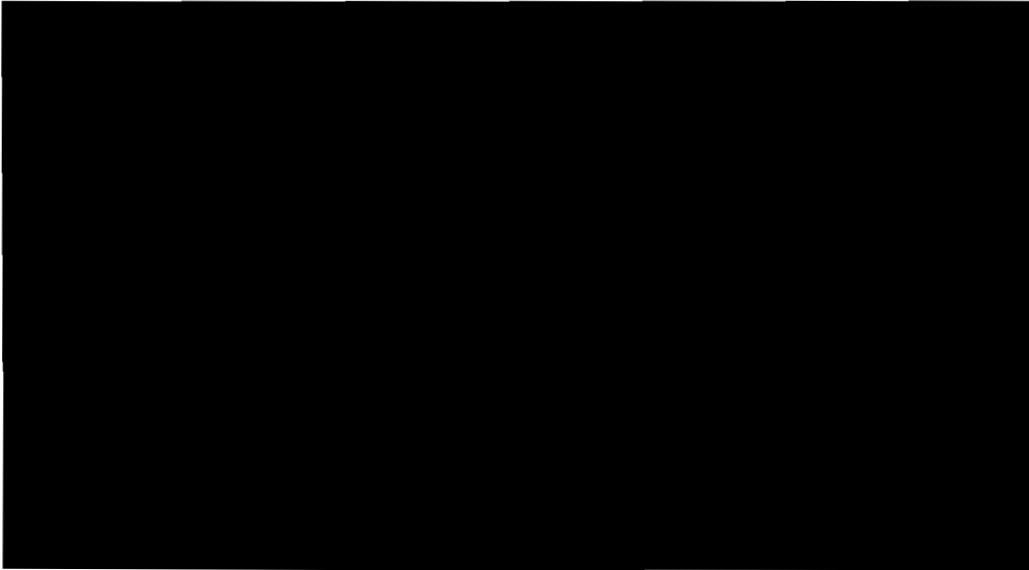
UNCLASSIFIED

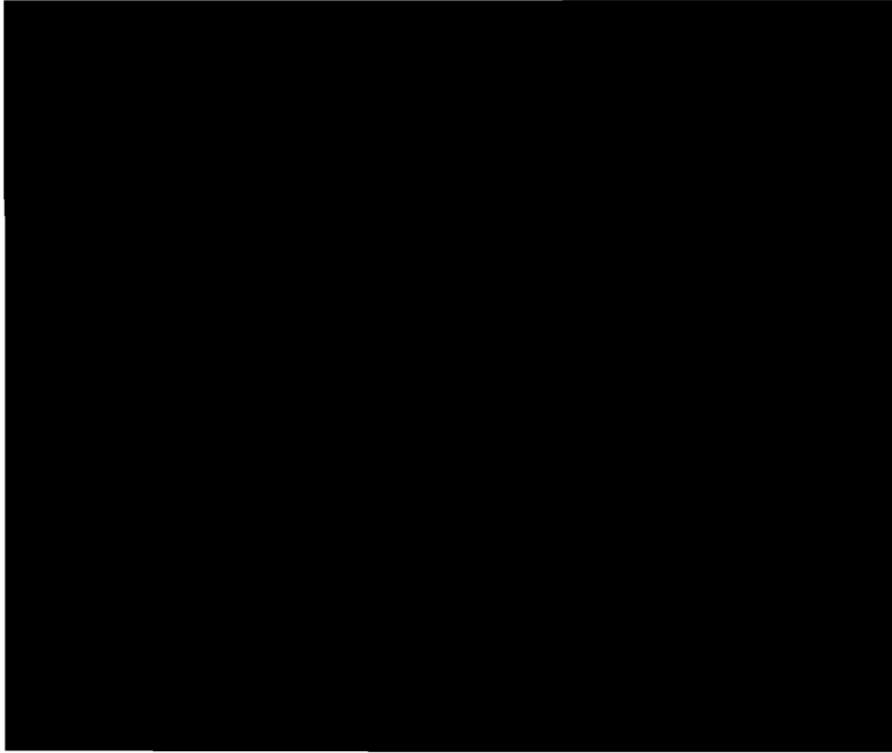
SENSITIVE BUT UNCLASSIFIED

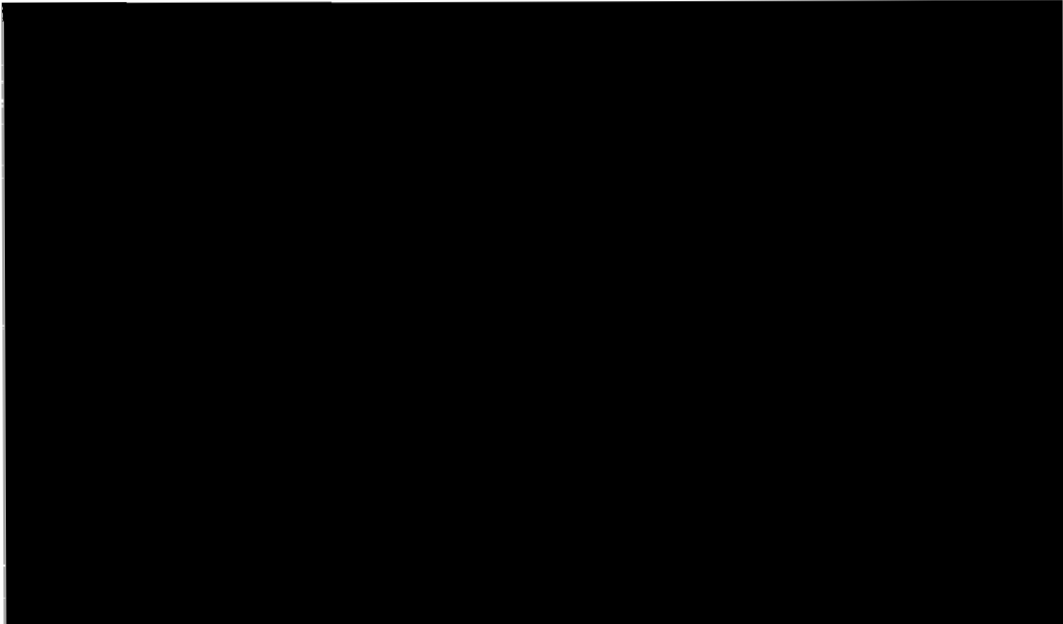
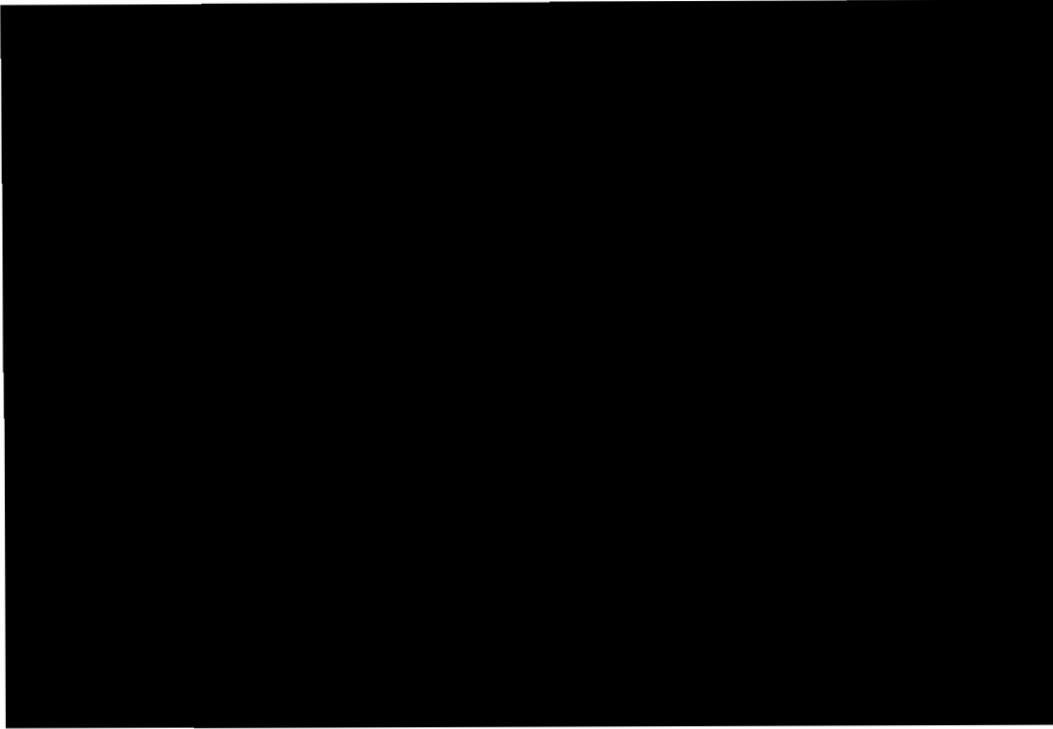


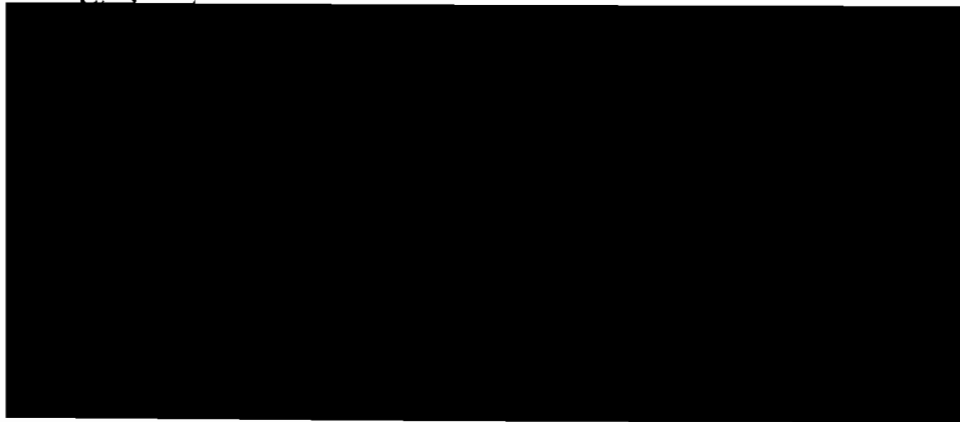
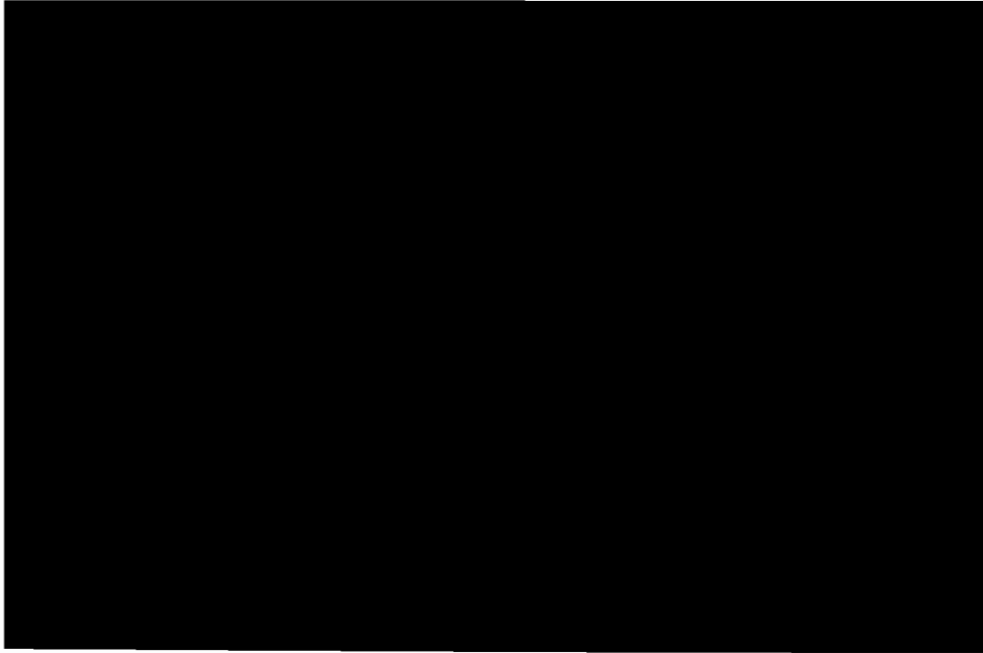




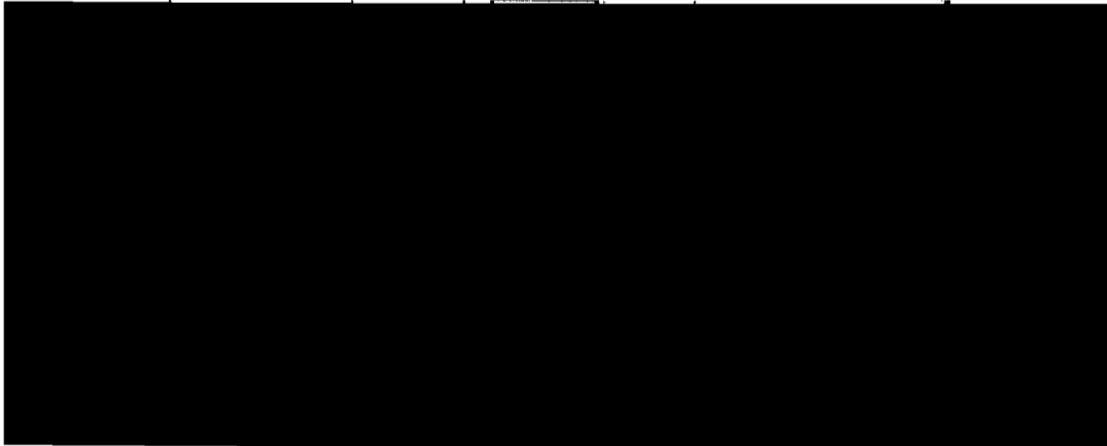
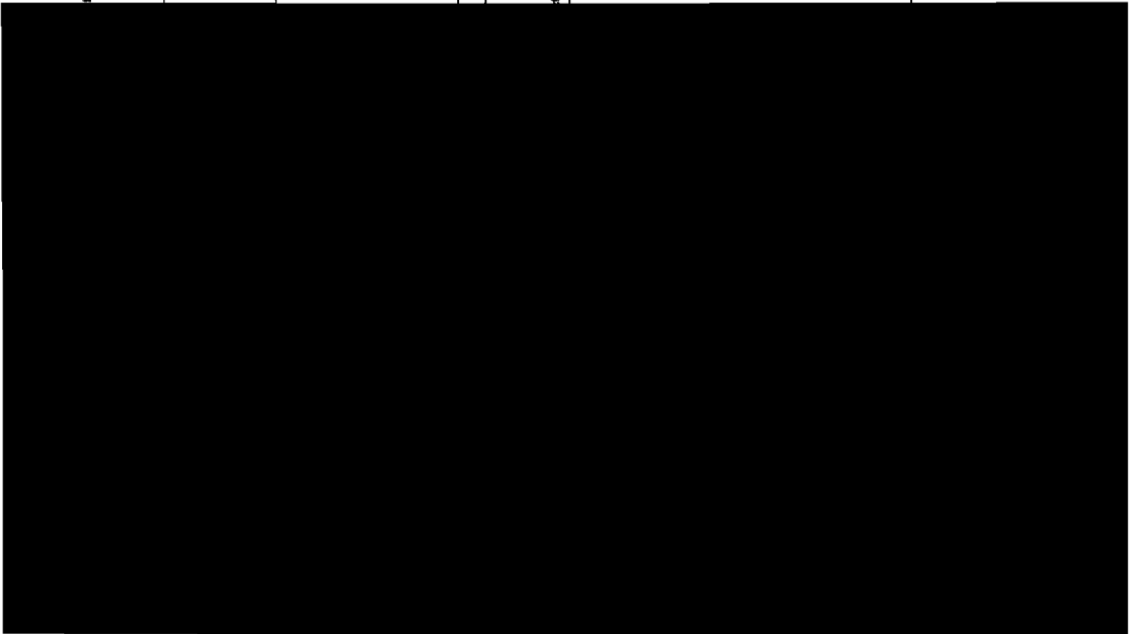
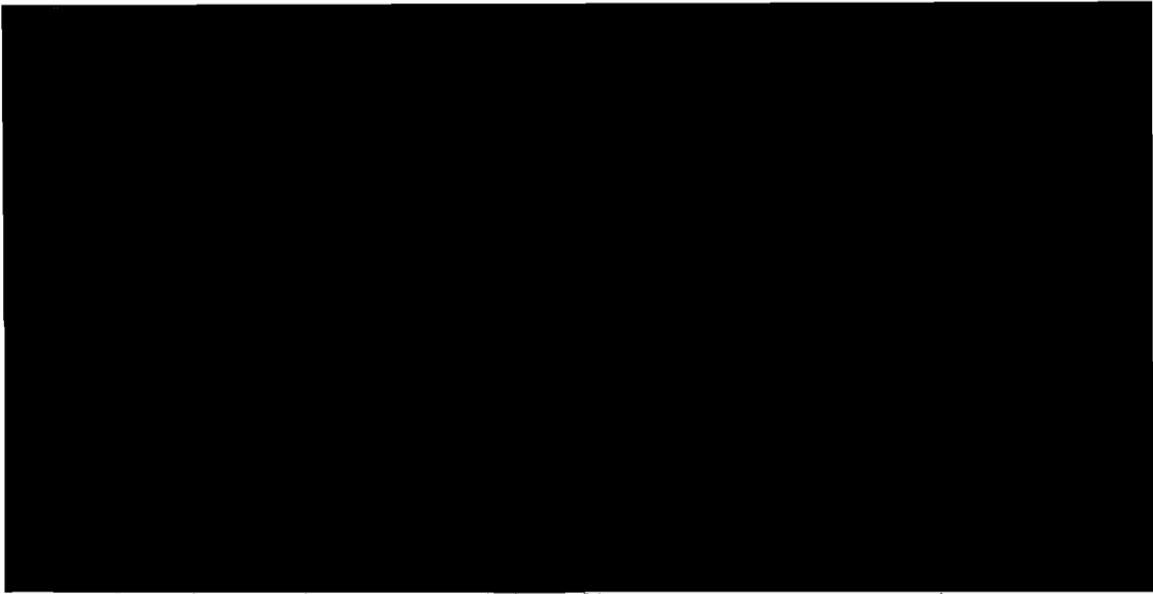




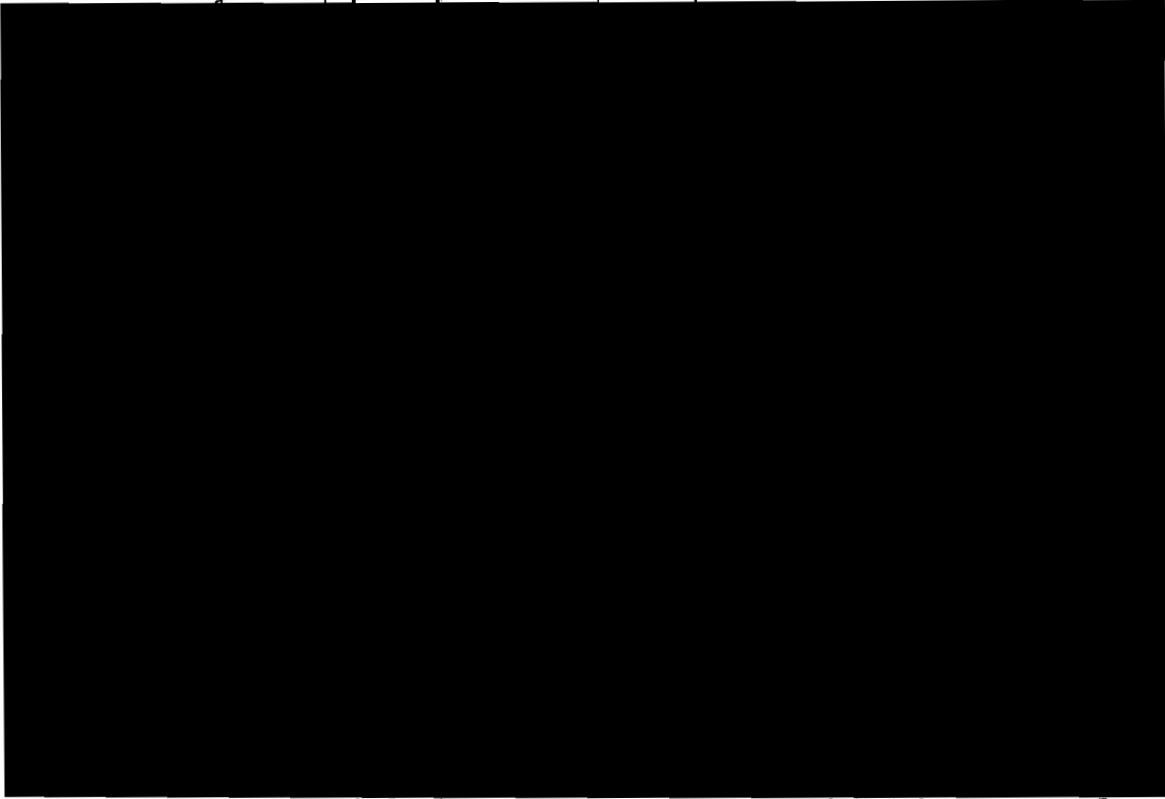
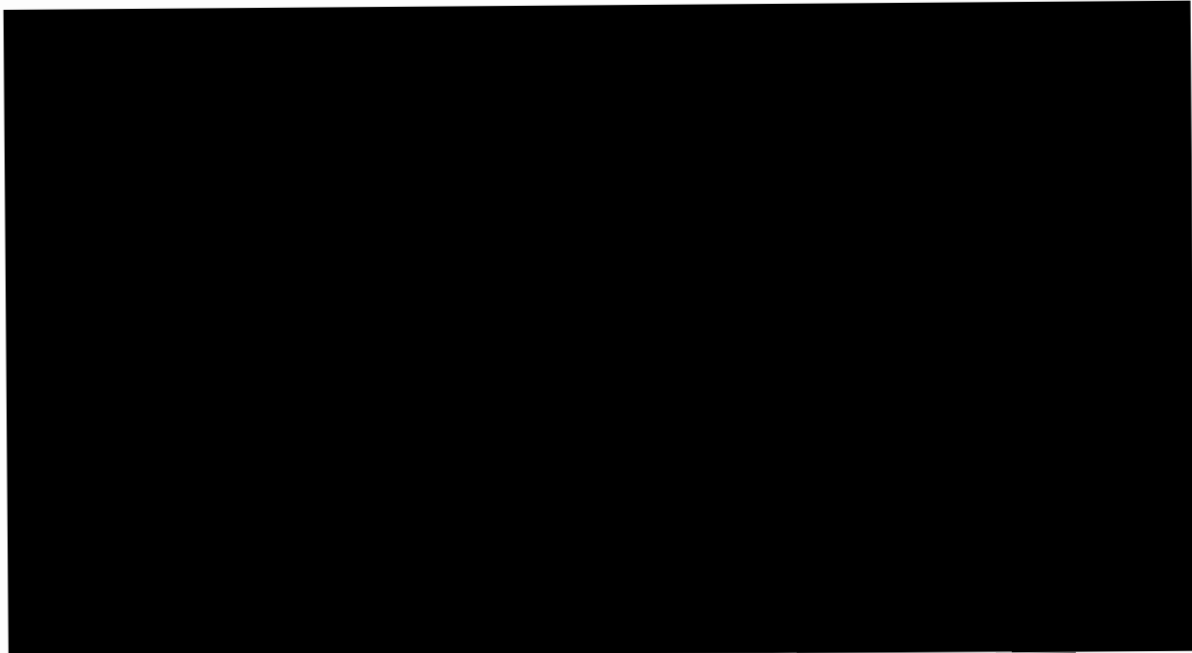


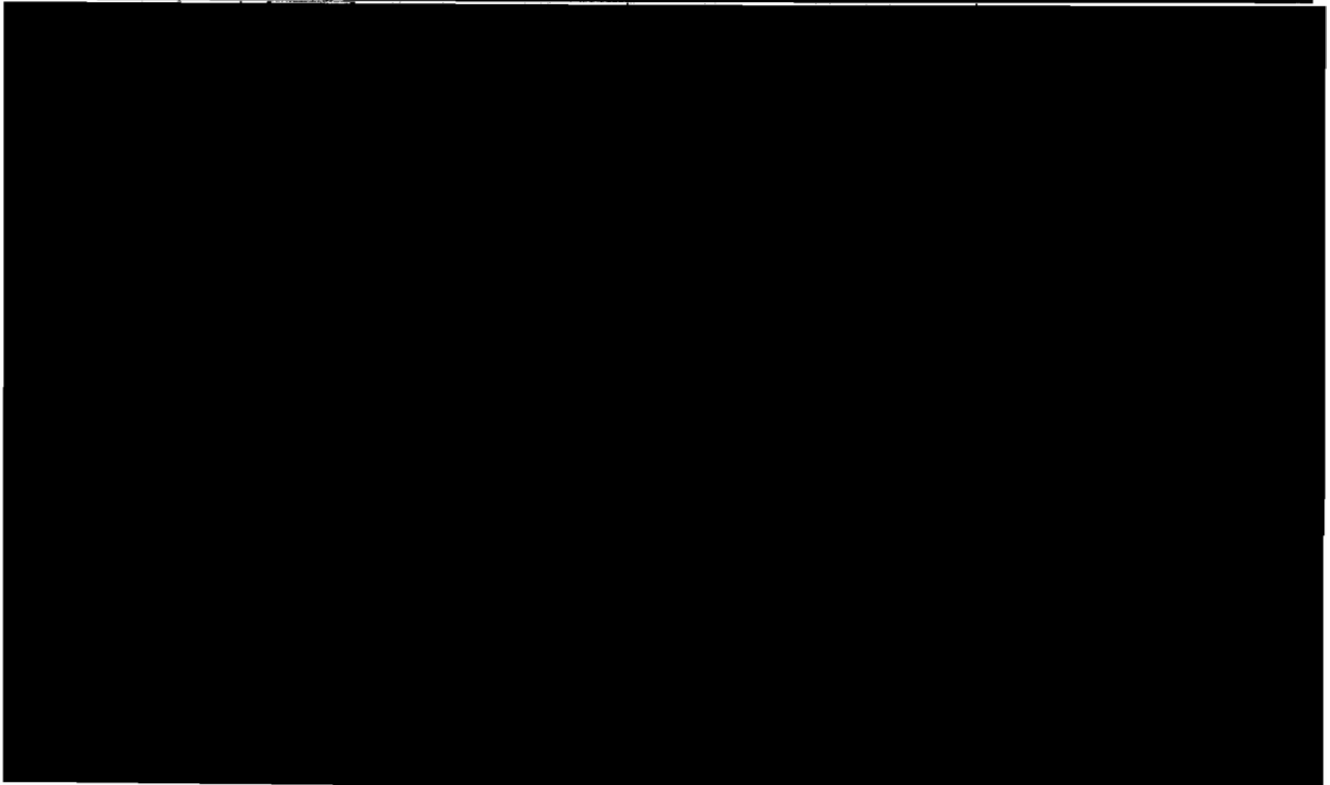
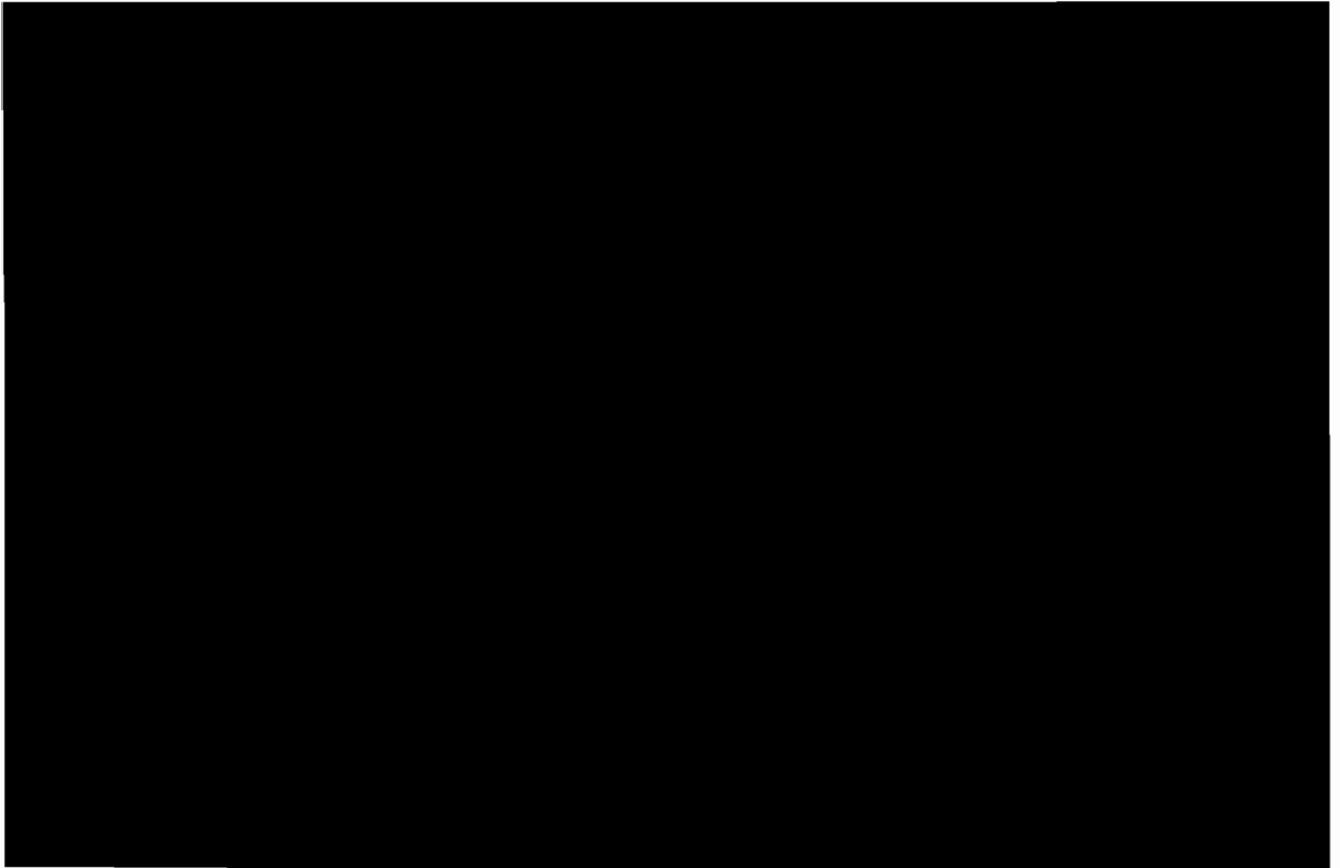


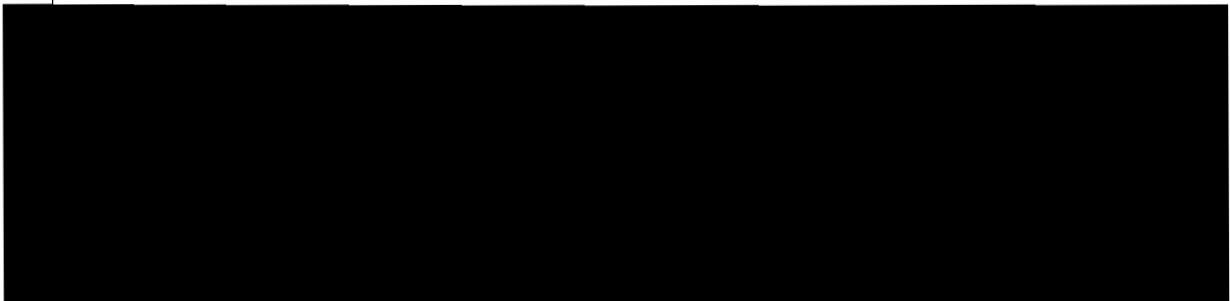
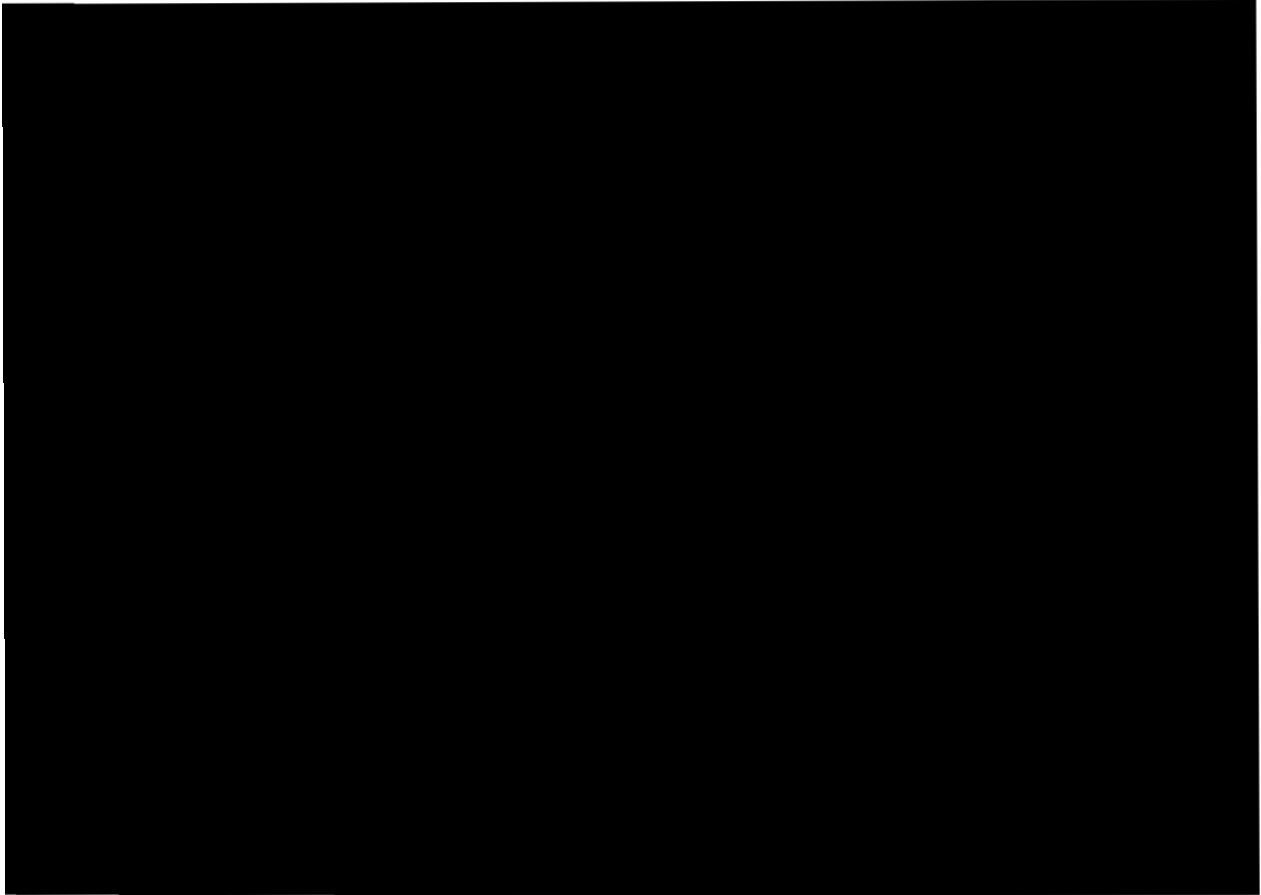
SENSITIVE BUT UNCLASSIFIED



SENSITIVE BUT UNCLASSIFIED







~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

APPENDIX E

Department's PII Breach Response Policy

United States Department of State



Personally Identifiable Information
**Breach Response
Policy**

Bureau of Administration

Incident Reporting, Response and Notification Procedures
for Breaches Involving Personally Identifiable Information

BACKGROUND

The policy contained herein sets forth a Department-wide approach when addressing breaches concerning personally identifiable information (PII) that is collected, processed, or maintained by the Department. This guidance is applicable to PII in any format (including paper and electronic) and is consistent with the prescribed framework in the Office of Management and Budget's Memorandum 07-16, entitled "Safeguarding Against and Responding to Breaches of Personally Identifiable Information."

The Department continues to respond to breaches involving the loss of PII. The most common causes of loss or potential compromise have involved the loss of paper records containing sensitive PII, e.g., social security numbers, etc. These losses are costly, time consuming and interfere with the Department's mission. They also create unnecessary risk of identity theft or other harms for our workforce and external stakeholders. Inasmuch as we compel the public and employees to provide information, we must make every effort to ensure the full protection of PII.

Because of the enormous amount of information that the federal government legitimately collects, uses, maintains and disseminates to accomplish its mission, data breaches are very difficult to prevent altogether. However, the Department will work to improve internal controls over the management and handling of PII and enhance privacy awareness on the part of our employees and contractors in order to minimize the risk of data breaches. In addition, the Department will implement policies to minimize the harm when such incidents do occur.

To address these and other privacy concerns, the Under Secretary of Management has established the Privacy Protection Governance Board (PPGB). The Assistant Secretary for Administration, as the designated Senior Agency Official for Privacy (SAOP), serves as the Chair of the PPGB, and will initiate several reviews to improve Department controls over PII. While improvements are being institutionalized, each and every Department employee and contractor must work diligently to reduce mishandling of PII, to protect PII in the Department's custody or control, and to respond swiftly when a breach does occur.

DEFINITIONS AND TERMS

The term “the Department” used herein means the Department of State.

“Personally identifiable information (PII),” with respect to an individual, is information which can be used to distinguish or trace an individual’s identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.

“Breach” is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

“Best judgment standard” refers to the need to assess in context the sensitivity of personally identifiable information and any actual or suspected breach of such information, for the purpose of deciding whether reporting a breach is warranted.

“Harm” means physical or fiscal damage, identity theft, personal or professional embarrassment, substantial inconvenience, unfairness, security risks, coercion, or other adverse effects on one or more individuals; or damage that undermines the integrity or confidentiality of a system or program.

“Confidentiality” means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

“Integrity” means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

“Identity theft” has the meaning given such term under section 603 of the Fair Credit Reporting Act (15 U.S.C. 1681a).

“Individual” is defined as a citizen of the United States; an alien lawfully admitted for permanent residence; a foreign employee or contractor of the Department or other U.S. federal agency; or person who is covered by an applicable international agreement between the United States and another country or an applicable agreement with another U.S. agency.

PURPOSE AND SCOPE

This policy addresses breaches of 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 or operated on behalf of the Department. Records pertaining to the issuance or refusal of visas or permits to enter the United States are not covered by this policy.

The foregoing policy does not supersede or supplant the requirements imposed by other laws, such as the Privacy Act of 1974.

RESPONSIBILITIES

The Assistant Secretary for Administration, as the Department's designated SAOP, has overall responsibility and accountability for ensuring the Department's implementation of information privacy protections in accordance with OMB Memorandum 06-15.

The Chief Information Officer is responsible for management of the Information Technology infrastructure for the Department.

The PPGB is responsible for addressing potential privacy issues impacting Department programs and initiatives and will oversee the organization and activities of various privacy-related working groups, such as the Data Breach Core Response Group (CRG).

The CRG will be convened at the discretion of the Privacy Office (A/ISS/IPS/PRV) or the Executive Secretary of the PPGB in the event of an actual or suspected breach involving PII, to determine whether the incident poses problems related to identity theft or risk of other harm, conduct a risk analysis, and direct an appropriate response.

A/ISS/IPS/PRV in the Bureau of Administration will oversee the Department's programs for protecting PII and reporting, and responding to PII breaches, to include periodic risk assessments, in accordance with OMB Memorandum 07-16, and identify areas of privacy-related vulnerabilities and risks that are common across domestic and overseas offices.

Bureaus and posts will direct their employees and contractors, in the event of an actual or suspected breach, to report the incident immediately to DS/SI/CS Computer Incident Response Team (DS-CIRT), in accordance

with this Breach Response Policy and any published bureau or post procedures. In the event of an actual or suspected breach involving PII under their custody, Bureau or post representatives will join the CRG to devise and implement an appropriate response.¹

The Bureau of Diplomatic Security (DS)

DS/CIRT, in the Office of Computer Security, will:

serve as the central point of contact for employees and contractors to report all suspected or confirmed PII loss or theft regardless of form, e.g. electronic or paper records.

notify the US Computer Emergency Readiness Team (US-CERT) within one hour of receiving a report of an actual or suspected breach of PII, after its determination that the suspected breach is reportable, using a best judgment standard.²

notify, as soon as possible after receiving a report of an actual or suspected breach of PII, A/ISS/IPS/PRV, which will determine if the CRG should be convened.

notify, as soon as possible the Office of the Inspector General (OIG) for any action that office deems appropriate.

provide technical support for inquiries into actual or suspected PII breaches on the Department's computer networks and report its findings, as appropriate, when so requested by the CRG.

The DS Office of Investigations and Counterintelligence (DS/ICI) will serve as the central point of contact for PII breaches involving paper records that require a DS investigation or any PII breach, e.g. electronic or paper records, where criminal activity is suspected.

¹ Bureaus are reminded to minimize the collection and retention of PII to that which is required to conduct business operations, and to ensure that PII is protected by appropriate safeguards to ensure security, confidentiality and privacy. Further direction on these and related matters will be forthcoming.

² Whether a breach should be reported will depend on a weighing of such factors as to whether the breach may result in harm to the individual, such as fiscal or physical damage, identity theft, personal or professional embarrassment, substantial inconvenience, unfairness, security risks, coercion, and/or any other adverse effects.

IDENTIFICATION AND REQUIRED REPORTING OF BREACHES

Upon a finding of an actual or suspected breach involving PII, Department employees and contractors must immediately report the breach to their manager and to DS-CIRT.

Examples of PII breaches that typically should be reported include, but are not limited to, those involving the following types of information, whether pertaining to employees or members of the public:

- Personnel or payroll information
- Social Security numbers and/or passport numbers
- Date of birth, place of birth and/or mother's maiden name
- Medical information
- Identifiable information concerning individuals who may be the subject of ongoing law enforcement investigations
- Department credit card holder information or other information on financial transactions (e.g., garnishments)
- Passport applications and/or passports
- Biometric records

If the employee or contractor determines that an incident should be reported, applying these standards, he or she must notify his or her manager and the DS/CIRT. DS/CIRT is staffed 24 x 7 and can be reached by unclassified email at CIRT@state.gov or telephone at (301) 985-8347.

The report should contain the following information about the loss, if known:

- (1) Contact information for individual making report;
- (2) Bureau/Post and office where breach occurred;
- (3) Nature/circumstances of breach;
- (4) Date/time of breach in local time (to include time zone);
- (5) Description of breached data;
- (6) Format of breached data (electronic or paper records);
- (7) If electronic, what equipment was involved, e.g. floppy disk, laptop, PDA, etc? Was the media encrypted? If yes, product used;
- (8) Is breach confirmed or suspected;
- (9) The actions, if any, taken to recover missing materials;

~~**SENSITIVE BUT UNCLASSIFIED**~~

- (10) How many individuals potentially affected;
- (11) Assessment of the risk of harm; and
- (12) The actions taken to mitigate potential harm.

DEPARTMENT RESPONSE TO PII BREACH

Upon receipt of a PII breach report, DS-CIRT, applying a best judgment standard, will notify US-CERT within one hour and notify A/ISS/IPS/PRV either beforehand or shortly thereafter. A/ISS/IPS/PRV will make a determination whether to convene the CRG to conduct a risk analysis.

RISK ANALYSIS

In conducting a risk analysis, the CRG will consider:

- (1) The nature and content of the breached data, e.g., the data elements involved, such as name, social security number, date of birth;
- (2) The ability and likelihood of an unauthorized party to use the lost, stolen or improperly accessed or disclosed data, either by itself or with data or applications generally available, to commit identity theft or otherwise misuse the data to the disadvantage of any person;
- (3) Ease of logical data access to the breached data in light of the degree of protection for the data, e.g., unencrypted, plain text;
- (4) Ease of physical access to the breached data, e.g., the degree to which the data is readily available to unauthorized access;
- (5) Evidence indicating that the breached data may have been deliberately targeted by unauthorized persons; and
- (6) Evidence that the same or similar data had been acquired in the past from other sources and used for identity theft or other improper purposes.

Upon conclusion of the risk analysis, the CRG will determine whether the Department should do any or all of the following:

- notify affected individuals;
- offer credit protection services to affected individuals;

~~**SENSITIVE BUT UNCLASSIFIED**~~

- notify an issuing bank if the breach involves government-authorized credit cards;
- review and identify systemic vulnerabilities or weaknesses and preventive measures; and
- take other measures to mitigate the potential harm.

The CRG will work with appropriate Bureaus to review and reassess, if necessary, the sensitivity of the breached data to determine when and how notification should be provided or other steps that should be taken. Any recommendation for notification shall be made by the CRG to the Chair of the PPGB, who may refer the matter to the full PPGB or, if necessary, the Under Secretary for Management. The Bureau of Resource Management shall be consulted on the cost implications of proposed mitigation measures. The Under Secretary of Management, pursuant to Delegation of Authority DA-198, or other duly delegated official, shall make final decisions regarding notification of the breach. Notification—including provision of credit monitoring services—also may be made pursuant to bureau-specific procedures that are consistent with this policy and OMB 07-16 requirements and that have been approved in advance by the PPGB and/or the Under Secretary for Management.

Should the CRG find, based upon a complete risk analysis, that there is minimal risk for the potential misuse of PII involved in a breach, it will advise the PPGB and take no further action unless the PPGB decides otherwise.

ACCELERATED NOTIFICATIONS

Nothing in this policy affects the Secretary's or the Under Secretary for Management's discretion to take whatever steps deemed necessary, consistent with applicable law, to respond to a breach of PII.

NOTIFICATION ELEMENTS

The following are guidelines for notifying individuals whose personal information is subject to a risk of misuse arising from a breach. Notification, typically under the signature of the appropriate Assistant Secretary, or appropriate official at post, should generally include the following elements, as appropriate:

SENSITIVE BUT UNCLASSIFIED

- (1) A brief description of what happened, including the date[s] of the breach and its discovery, if known;
- (2) To the extent possible, a description of the types of personal information that were involved in the breach (e.g., full name, Social Security number, date of birth, home address, account numbers);
- (3) A brief description of what the Department is doing to investigate the breach, to mitigate harm, and to protect against any further breach of the data;
- (4) Contact procedures for those wishing to ask questions or learn additional information, which will include a toll-free telephone number, an e-mail address, Web site, and/or postal address;
- (5) Steps individuals should take to protect themselves from the risk of identity theft, including steps to obtain fraud alerts (alerts of any key changes to such reports and on-demand personal access to credit reports and scores), if appropriate, and instructions for obtaining other credit protection services, such as credit freezes; and
- (6) A statement whether the information was encrypted or protected by other means, when determined that such information would be beneficial and would not compromise the security of the system.

In developing a mitigation strategy, the Department will carefully consider all available Credit Protection Services and extend such services in a consistent and fair manner. Affected persons will be advised of the availability of such services, where appropriate under the circumstances, in the most expeditious manner possible, including but not limited to mass media distribution and broadcasts.

SENSITIVE BUT UNCLASSIFIED

MEANS OF NOTIFICATION

Notification by first-class mail should be the primary means by which notification is provided. In instances where there is insufficient, or out-of-date contact information that precludes direct written notification to an individual who is the subject of a data breach, a substitute form of notice may be provided, such as a conspicuous posting on the home page of the Department's Web site and notification in major print and broadcast media, including major media in geographic areas where the affected individuals likely reside. Such a notice in media will include a toll-free phone number where an individual can learn whether or not his or her personal information is possibly included in the breach. Special consideration for accommodations should be consistent with Section 508 of the Rehabilitation Act of 1973 and may include the use of telecommunications devices for the deaf or hard of hearing.

Should it be determined that notification must be immediate, the Department may provide information to individuals by telephone or other means, as appropriate.

Notwithstanding the foregoing, notifications may be delayed or barred upon a request from the Bureau of Diplomatic Security or other Federal agencies in order to protect data, national security or computer resources from further compromise or to prevent interference with the conduct of a lawful investigation or efforts to recover the data.

Any request for delay in notification of the affected subjects should state an estimated date after which the requesting entity believes that notification will not adversely affect the conduct of the investigation, national security, or efforts to recover the data. Any delay should not exacerbate risk or harm to any affected individuals. The PPGB must be informed of a delayed notification.

RULES AND CONSEQUENCES

Employees and contractors will be held accountable for their individual actions. In certain circumstances, consequences for failure to properly safeguard PII or to respond appropriately to a breach could include disciplinary action; also, such failure could be addressed in individual

performance evaluations. Supervisors who are aware of PII breaches by their subordinates and allow such conduct to continue may also be held responsible for failure to provide effective organizational security oversight.

DOCUMENTATION OF BREACH NOTIFICATION RESPONSES

The Bureau of Administration, as appropriate, shall document the Department's responses to breaches and shall ensure that appropriate and adequate records are maintained. These records shall be maintained in accordance with applicable law.

EVALUATION OF BREACH RESPONSES

The development and implementation of this policy is an ongoing process. Accordingly, it will be evaluated after the reporting of suspected or actual breaches to identify tasks that could have been conducted more effectively and efficiently and to make improvements and modification as appropriate.

Nothing in this policy creates any right enforceable against the Department.

~~**SENSITIVE BUT UNCLASSIFIED**~~

~~**SENSITIVE BUT UNCLASSIFIED**~~

APPENDIX F

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) |

| Federal Requirements (General) | |
|---|--|
| Computer Fraud and Abuse Act 18 U.S.C. § 1030 | <p>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:</p> <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 |
| OMB Memorandum M 07 16, “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”* (May 22, 2007) | <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. |

| Federal Requirements (General) | |
|---|--|
| OMB A-130 (Revised), Management of Federal Information Resources (Transmittal Memorandum #4, 11/28/2000) | This circular requires agencies to: <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. |
| NIST Special Publication 800-53 (Revision 2), Recommended Security Controls for Federal Information Systems (December 2007) | 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. <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.

| 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. |

| 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.] |

| Department Requirements for Protecting Passport Records | |
|--|--|
| Notice To All Employees of Passport Services: Privacy Reminder (Bureau of Consular Affairs, March 25, 2008) | This Bureau of Consular Affairs notice was issued to emphasize: <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. |
| Interim Reporting Guidelines for Incidents of Unauthorized Access to Passport Records/Applicant Personally Identifiable Information (Bureau of Consular Affairs, April 9, 2008) | 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) |
| Personally Identifiable Information Breach Response Policy (Bureau of Administration, May 1, 2008) NOTE: Although approved, this policy had not been issued as of May 14, 2008. | 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) |

APPENDIX G

Bureau of Consular Affairs Response



United States Department of State

Assistant Secretary of State
for Consular Affairs

Washington, D.C. 20520

SENSITIVE BUT UNCLASSIFIED

June 20, 2008

TO: OIG/AUD - Mark W. Duda

FROM: CA – Janice Jacobs

SUBJECT: 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), dated June 5, 2008

Attached is CA's response to your office's June 2008 Final Report on *Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System (PIERS)*. We appreciate your insights, and CA is well on the way to implementing your recommendations.

We are sobered by the seriousness of your findings. This report shows we have more work to do to ensure that we are protecting the personal information Americans entrust to us when they apply for passports. We continue to believe that many of these accesses were motivated by the imprudent curiosity of employees who made bad decisions, contrary to existing Department policy.

However, since we became aware of these vulnerabilities in March of 2008, we have already undertaken a number of initiatives in both the short and long term to mitigate the vulnerabilities to unauthorized access of passport records. Many of the short term fixes/corrective actions are detailed in the Exhibit to Appendix C of your draft report.

For the long term, CA is committed to providing the appropriate safeguards for the personally identifiable information (PII) provided with each passport application for every U.S. citizen. We have formed a working group comprised of representatives from across the Department to formulate ideas, gather requirements, and take action in developing systems solutions in several core areas. The group is currently engaged to vastly improve the way we monitor access to

SENSITIVE BUT UNCLASSIFIED

passport records, upgrade our auditing capabilities, provide feedback on the trends and methods systems users follow to access passport data, modernize our reporting mechanisms when we are alerted to a possible case of unauthorized access, improve our overall training with regards to privacy and protecting PII, and ensure CA applies consistent disciplinary procedures when incidents of unauthorized access occur.

I am confident that these improvements will enhance the overall security of the passport records.

My staff is prepared to answer any additional questions at anytime. The Bureau points of contact are Barry Conway, Director, Office of Passport Integrity and Internal Controls, and Gail Neelon, Director, Office of Legal Affairs and Law Enforcement Liaison. They may be reached at 663-2403 and 663-2427, respectively.

Attachment:

CA Responses to 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), dated June 2008

SENSITIVE BUT UNCLASSIFIED

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

List of Recommendations

Recommendation 1: OIG recommends that the Bureau of Consular Affairs develop a mechanism to be able to accurately, readily, and, on a recurring basis, identify the universe of all PIERS user accounts, including the organization of the user.

CA Response: CA agrees with this recommendation.

In recognition of this vulnerability, CA conducted a complete review of all PIERS user accounts in May 2008. In addition to disabling inactive accounts, we also disabled those accounts that were missing key contact information. Going forward, CA will review the PIERS user accounts on a quarterly basis (minimum) to identify any inactive accounts or those accounts with deficient contact information.

Recommendation 2: OIG recommends that the Bureau of Consular Affairs (a) review all Department and non-Department PIERS user accounts within 60 days of the issuance of this report to identify all accounts that have been inactive for 90 days or more and accounts with incomplete or unknown identification information and (b) immediately determine whether these accounts are valid and have a current need for access. Those inactive accounts determined to have a valid need should be updated with correct and current user and access information, and those accounts determined not to have a valid need should be immediately deactivated and removed to avoid reactivation.

CA Response: CA agrees with this recommendation.

In May 2008, CA reviewed all PIERS user accounts and disabled those PIERS user accounts that had not been accessed within the last 90 days. This action resulted in disabling 14,895 accounts, leaving 10,115 active accounts. Of the 10,115 active accounts, CA next disabled those accounts that were missing the name or missing

key pieces of contact information (i.e. telephone #, email address, office location, office symbol). This action allowed CA to disable an additional 214 accounts.

Requirements to enhance the User Manager tool in PIERS are being developed to enhance its functionality. A new tool will require certain data fields to be entered before an account can be created. Specific reporting requirements have been identified to address deficiency in user activity reporting (i.e., number of active vs. inactive accounts, active accounts by organization, etc.).

Recommendation 3: OIG recommends that the Bureau of Consular Affairs, within 60 days of the issuance of this report, identify and validate all certifying authority officials and update their contact information as needed. Those officials found to no longer have a need for this designation should be immediately deactivated and removed from CCD and PIERS user authorization capability.

CA Response: CA agrees with this recommendation.

CA has initiated a review of all certifying authority officials. CA is working with the Consular Consolidated Database (CCD) administrators to generate a list of certifying authority officials with their contact information. If there is an email address in the contact information, we will email the certifying authority and ask them to revalidate their designation. If there is no email address, we will phone them. Those with no contact information will be disabled. CA will also generate a list of all Consular System and Technology (CST) managers at all posts and request they revalidate their role as a (CST) manager. CA will need 120 days to complete this recommendation.

Recommendation 4: OIG recommends that the Bureau of Consular Affairs, in coordination with PIERS certifying authorities, verify the accuracy, completeness, and business need for all active Department and non-Department user accounts within 90 days of the issuance of this report. Those accounts determined to have a valid need should be updated with correct and current user and access information, and those accounts determined not to have a valid need should be immediately deactivated and disabled from reactivation.

CA Response: CA agrees with this recommendation.

Once the certifying authority list is validated, we will provide each with a list of the users they have verified and ask them to validate the users and their access information. For post, we will request that the CST manager perform this revalidation and, for passport agencies/centers, we will request that the Information Systems Security Officer (ISSO) perform this revalidation. CA will need 180 days to complete this recommendation.

Recommendation 5: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures to ensure that system user accounts and certifying authority officials are reviewed on a quarterly cycle, or at least annually, in accordance with the minimum requirements contained in the National Institute of Standards and Technology (NIST) Special Publication 800-53.

CA Response: CA agrees with this recommendation.

In the short term, CA implemented a PIERS user access request policy at all passport agencies and centers. We developed draft requirements for a system-wide user access program. The User Manager enhancements to this program will address the need to review accounts on a quarterly or annual cycle. A reporting tool for this program will give us the ability to run user account reports on ad-hoc and quarterly bases. In the long term, CA will investigate automated methodologies to further accomplish the goals of this recommendation.

Recommendation 6: OIG recommends that the Bureau of Consular Affairs develop and provide periodic training to certifying authority officials. The training should emphasize the importance of the officials' responsibilities, including the need to verify user information prior to granting access to the system and deactivating accounts as appropriate.

CA Response: CA does not concur with this recommendation in its entirety.

CA/PPT is in the process of evaluating procedures for certifying authorities. We plan to implement, at a minimum, an annual signed statement from each certifying authority official affirming their understanding of their role and responsibilities in addition to verifying the validity of their user information. CA believes that the basic duties and responsibilities can be conveyed effectively in this manner, whereas creating a training class would not be cost effective. These procedures will be affirmed in revisions to the current MOU's with federal agencies we share PIERS access.

Recommendation 7: OIG recommends that the Bureau of Consular Affairs (a) in coordination with the Foreign Service Institute, stop providing access to actual PIERS data for training sessions and develop an alternative approach, such as simulated PIERS data with fictional records, and (b) determine whether access to actual data is provided in other training environments, including at other agencies and contractor venues, and replace with simulated PIERS data.

CA Response: CA agrees with this recommendation.

CA is in the process of generating a test data version of the PIERS database. We have identified commercial off the shelf software to generate the test data and are in the process of working with the A Bureau Privacy Office to identify the fields that need to be modified and/or altered. Once we generate the test data base, it will be available for all authorized OpenNet users.

Recommendation 8: OIG recommends that the Bureau of Consular Affairs consider the types of controls that the Treasury Inspector General for Tax Administration, the Internal Revenue Service, and the Social Security Administration have put in place to protect electronic personally identifiable information and develop and implement a comprehensive and coordinated strategy for proactively preventing and detecting incidents of unauthorized access to PIERS.

CA Response: CA agrees with this recommendation.

The Working Group that CA convened in March 2008 met with representatives from the Internal Revenue Service, the Social Security Administration, and the Department of Veteran's Affairs in April to ascertain their best practices and lessons learned related to unauthorized access of PII, their auditing systems, and reporting procedures. All three entities provided valuable information that CA is using in developing long range initiatives for monitoring, auditing, and reporting incidents of unauthorized access.

Recommendation 9: OIG recommends that the Bureau of Consular Affairs develop a complete PIERS business requirements implementation plan that covers all aspects—such as guidance, training, verification, violations, and agreements with other agencies—before executing the new tiered-access levels.

CA Response: CA agrees with this recommendation in part.

CA has already completed the business requirements for tiered level access for federal agency PIERS access. The project is currently in development with a tentative completion date of Fall 2008. CA believes that the business requirements implementation plan can be efficiently done in tandem with these new levels of access. The tiered levels of access were thoroughly vetted with the Department and our outside agency partners. Waiting for completion of the implementation plan will only delay a critical mitigation mechanism to safeguard against unauthorized access. Performing these functions in tandem provides system agility that will enable CA to expand and /or contract the levels of access in real time.

Recommendation 10: OIG recommends that the Bureau of Consular Affairs (CA) conduct an analysis of PIERS passport records frequently accessed by users to determine trends and excessive hits on an individual's records and to make appropriate additions to the listing of individuals contained in Monitor. From this analysis, the Bureau should develop guidance for periodically updating the names of individuals in Monitor.

CA Response: CA agrees with this recommendation.

CA is currently drafting standard operating procedures to dictate the rules and methods to add and delete individuals from the Monitor List. We also plan to conduct coordinated PIERS user analysis with CST and Passport Services Office of Technical Operations (CA/PPT/TO). This analysis will ensure that the Monitor List contains the appropriate passport records and will implement a reporting mechanism and system alerts to identify violators who access records that are part of the Monitor List.

Recommendation 11: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for investigating access alerts generated by Monitor and develop an independent means to identify why an access was made, such as by adding a mandatory field in PIERS to capture the reason for access.

CA Response: CA agrees with this recommendation.

In April 2008, as a result of the efforts of the Working Group that was formed to mitigate the vulnerabilities to unauthorized access, Passport Services implemented

revised interim procedures for reporting and investigating potential instances of unauthorized access. Various bureaus within the Department contributed to these new procedures, to include Diplomatic Security (DS), OIG, the Office of the Legal Advisor (L), and the Bureau of Administration (A Bureau). Working with these bureaus ensured that their needs and concerns were addressed and resulted in Department-coordinated reporting and investigation procedures.

In addition, CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. CA is committed to providing the necessary resources to develop a mandatory drop-down selection for entry into PIERS, requiring the user to provide a reason for their use of the database. CA believes this will act as a deterrent to unauthorized access. CA is also working with the A Bureau to build a comprehensive alert system that will better leverage technology and enhance the interim reporting procedures already in place.

Recommendation 12: OIG recommends that the Bureau of Consular Affairs conduct an assessment to determine the appropriate level of resources needed to effectively receive, investigate, and verify alerts for potential unauthorized access generated by Monitor.

CA Response: CA agrees with this recommendation.

Since the incidents of unauthorized access, CA has provided and will continue to provide the necessary staffing resources to the office currently responsible for overseeing the monitoring function of the PIERS database. We are currently assessing the long term needs of this office based on the short and long term initiatives being implemented.

Recommendation 13: OIG recommends that the Bureau of Consular Affairs develop a method and mechanism to periodically review all PIERS user accounts for indicators of potential unauthorized access to passport records, including performing periodic audits of the existing automated activity logs available in PIERS to identify when and what records were accessed, and data mining techniques to identify trends in user accesses to individual passport holder records.

CA Response: CA agrees with this recommendation.

In the short term, CA has implemented a formal audit program for all PIERS users within Passport Services. The audits are performed monthly by a passport agency's senior management to review both the permissions for personnel to have access to PIERS and the actual queries the employees conduct in PIERS. These audits started in April 2008 and will be done at least once a year for every employee. In addition, CA/CST is developing randomly generated lists of PIERS users for both non-Passport Services employees and PIERS users from other agencies, so random audits can also be conducted.

In the long term, CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. The working group convened by CA (mentioned above) will address the



Recommendation 14: OIG recommends that the Bureau of Consular Affairs develop and implement policies and procedures for quality assurance that require certifying authorities to verify user and supervisor contact information for completeness and accuracy before they grant users access to the passport systems and to confirm periodically the continuing need for the access.

CA Response: CA agrees with this recommendation.

CA is in the process of gathering requirements to improve the overall security of systems and databases that contain PII from passport applications. The working group will also address the issue of managing and tracking certifying authority information. In addition, the MOU's with federal agencies will be reviewed and strengthened so the requirements for certifying authorities are detailed.

Recommendation 15: OIG recommends that the Bureau of Consular Affairs (a) perform a technical and cost analysis for adding a required drop-down selection or field in PIERS to force users to identify the reason specific passport records need to be accessed and (b) identify the necessary resources to develop and implement such capability in PIERS.

CA Response: CA agrees with this recommendation.

See response to Recommendation #11.

Recommendation 16: OIG recommends that the Bureau of Consular Affairs (CA), in coordination with the Bureau of Administration, ensure that (a) CA's policy and the Department of State's breach notification policies, procedures, and guidance are consistent to effectively address incidents of unauthorized access of passport records and (b) the final versions of each document are promptly incorporated into the applicable Foreign Affairs Manual and Foreign Affairs Handbook.

CA Response: CA agrees with this recommendation.

CA has and will continue to coordinate with the Bureau of Administration on all policies and procedures developed to mitigate the vulnerabilities to unauthorized access of passport records so they are in synch with A Bureau's Breach Response Policy. CA will also ensure any new policy or procedure is incorporated into the Foreign Affairs Manual and Foreign Affairs Handbook on a timely basis.

Recommendation 17: OIG recommends that the Bureau of Consular Affairs, in coordination with the Bureau of Human Resources, develop and implement specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information. This guidance should address all passport system users, including contractors, from the Department and other agencies.

CA Response: CA does not concur with this recommendation.

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.

Recommendation 18: OIG recommends that the Bureau of Consular Affairs ensure the accuracy of its Privacy Impact Assessments (PIAs) 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.

CA Response: CA agrees with this recommendation.

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.

Recommendation 20: OIG recommends that the Bureau of Consular Affairs develop policies and procedures that address third-party disclosure requirements and breaches, to include disciplinary actions to be taken in response to inappropriate disclosures.

CA Response: CA agrees with this recommendation.

CA/PPT is in the process of evaluating all of the current MOU's with the federal agencies that are granted access to the PIERS database, or are provided information from it, to ensure the proper provisions are in place to detail the procedures to follow for disclosing information to third parties and the actions to take if information is provided without State approval/consent. CA will also ensure appropriate cases are coordinated for investigation as warranted.

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:

SENSITIVE BUT UNCLASSIFIED

- 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 read and understand the Privacy Act and their obligation to safeguard passport records and the privacy of passport applicants;
- annual training for and responsibilities of certifying authorities, including disabling access/deactivating users accounts immediately, when access is no longer merited;
- specific guidance, criteria, and requirements to ensure that agencies provide only the level of access required by each user when tiered-access to PIERS is implemented;
- oversight responsibilities for all appropriate Department and other agency officials to ensure that access levels are properly assigned and maintained;
- the agency's responsibilities for preventing, detecting, and reporting breaches and the Department's rights when the Department detects possible breaches made by other agency personnel; and
- minimum actions (such as deactivation of access) for identified violators who either access records improperly or authorize unnecessary levels of access.

CA Response: CA agrees with this recommendation.

CA/PPT is in the process of evaluating all of the current MOU's with the federal agencies that are granted access to the PIERS database and reaching out to the various points of contact for each MOU. CA plans to amend each MOU so each action item above is incorporated.

Recommendation 22: OIG recommends that the Bureau of Consular Affairs (CA) ensure that the addendum to the Memorandum of Agreement with the Department of Homeland Security (DHS) regarding the transfer of PIERS and passport data to DHS contains, at a minimum, elements to:

- clearly identify how and by whom the data will be used;
- specify the actions to be taken against DHS should it misuse or fail to properly protect the data; and
- address specific requirements to ensure that—

SENSITIVE BUT UNCLASSIFIED

- o the data is adequately protected,
- o any unauthorized and/or inappropriate access or disclosure of passport information is detected and reported to appropriate officials in CA and DHS, and
- o users who commit an unauthorized access to or inappropriate disclosure of passport data are held accountable to a minimal level that is at least comparable to CA and Department standards.

CA Response: CA agrees with this recommendation.

CA has been working extensively with DHS for years to find better ways to improve the flow of information from passport records to their personnel in the field so they can make better judgments at border crossings with regards to the legitimacy of travel documents and thus improve overall border security. Part of this initiative was to transfer appropriate passport record data directly to DHS. Based on the incidents of unauthorized access, CA is re-assessing the proposed procedures to ensure the requirements listed above are part of the MOU and day to day processes.

SENSITIVE BUT UNCLASSIFIED

SENSITIVE BUT UNCLASSIFIED

APPENDIX H

Bureau of Administration Response

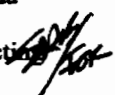


United States Department of State
Assistant Secretary for Administration
Washington, D.C. 20520

UNCLASSIFIED

MEMORANDUM

TO: OIG/AUD – Mark W. Duda

FROM: A – William H. Moser, Acting 

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

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 Assessments*. 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.

Recommendation 16: OIG recommends that the Bureau of Consular Affairs (CA), in coordination with the Bureau of Administration, ensure that (a) CA's policy and the Department of State's breach notification policies, procedures, and guidance are consistent to effectively address incidents of unauthorized access of passport records and (b) the final versions of each document are promptly incorporated into the applicable Foreign Affairs Manual and Foreign Affairs Handbook.

Response to Recommendation 16: The Bureau of Administration (A) concurs with the recommendation that the Bureau of Consular Affairs, as well as all Department components, work in close coordination with the A Bureau to ensure consistency in all privacy policies, including incident reporting, training, and operational matters. The Department's Breach Response Policy serves as the overall guidance for addressing incidents of unauthorized access and will be incorporated into the Foreign Affairs Manual and Foreign Affairs Handbook.

APPENDIX I

Bureau of Human Resources Response



United States Department of State

Bureau of Human Resources

Washington, D.C. 20522

June 16, 2008

MEMORANDUM

TO: IG – Mr. Harold W. Geisel, Acting

FROM: DGHR – Harry K. Thomas, Jr. 

SUBJECT: Draft Report: "Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System"

Thank you for the opportunity to respond to the draft audit entitled "Review of Controls and Notification for Access to Passport Records in the Department of State's Passport Information Electronic Records System". We note that the Bureau of Human Resources (HR) is participating in one recommendation. I have several comments to offer regarding recommendation 17 which proposes that we develop and implement specific disciplinary guidelines and a table of disciplinary actions and penalties to address unauthorized access to passport information.

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.

I hope my comments are helpful as you finalize the report.

APPENDIX J



Foreign Service Institute Response

United States Department of State

Foreign Service Institute

George P. Shultz National Foreign Affairs Training Center
Washington, D.C. 20522-4201

June 12, 2008

MEMORANDUM

TO: OIG/AUD – Mr. Mark W. Duda

FROM: FSI/EX – Catherine J. Russell

SUBJECT: FSI Comments re Draft Report on *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 on the subject draft Audit Report. FSI provides the following comments and suggested edits.

Recommendation 6: OIG recommends that the Bureau of Consular Affairs develop and provide periodic training to certifying authority officials. The training should emphasize the importance of the official's responsibilities, including the need to verify user information prior to granting access to the system and deactivating accounts as appropriate.

FSI's Consular Training Division currently provides training to DOS certifying authorities (CST Administrators) during the mid-level Automation for Consular Managers course (PC-116), which is offered 12 times a year. The segment includes a discussion of CA policy as well as hands on training in assigning appropriate roles to both consular and non-consular employees, such as RSOs and DCMs.

FSI is currently developing a Passport Data Security distance learning course for CA which will provide initial and annual certification not just for certifying authorities, but for all PIERS users. FSI is working closely with CA to determine the best method of delivery for this course.

Recommendation 7: OIG recommends that the Bureau of Consular Affairs (a) in coordination with the Foreign Service Institute, stop providing access to actual PIERS data for training sessions and develop an alternative approach, such as simulated PIERS

~ 2 ~

data with fictional records, and (b) determine whether access to actual data is provided in other training environments, including at other agencies and contractor venues, and replace with simulated PIERS data.

The three ACS "roles" which we assign to our ConGen students enable them to perform a number of ACS functions, including managing a crisis, creating passports and reports of birth and processing subsistence loans and death cases. These roles also afford them PIERS access. FSI has requested that CA/CST remove PIERS from the student profile, preventing the possibility that the students will access the system without a need to know. FSI is exploring the possibility of creating a Passport Training Database using simulated PIERS records. The only PIERS activity currently included in ConGen is when the students are told to search for their own records in the system. During this session, the instructors take the opportunity to emphasize that the data is Privacy Act-protected and that there is a monitoring system in place. This could be accomplished using a training database. In addition, simulated PIERS data would allow us to incorporate passport record verification into other parts of our Americans Citizens Services module.

FSI strongly objects to inaccurate information included on page 12 of the draft report, which suggests that students were encouraged as a class to access the PIERS records of "prominent individuals." Far from encouraging such access, the lesson is used to emphasize the constraints of the Privacy Act. The instructor of the class in question has stated that he has never and would never instruct or suggest that a class look up the passport records of prominent individuals or celebrities. The allegation appears to be based on the comments of one student. Without corroboration from a significant number of other students in the course, FSI requests that the paragraph and other references to this unsubstantiated allegation be deleted.

If you have any questions regarding the above or need additional input from FSI, please feel free to contact Wayne Oshima in FSI/EX on x26730 or via unclassified e-mail (oshimawa@state.gov).

APPENDIX K

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.

~~SENSITIVE BUT UNCLASSIFIED~~

~~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.